Introduction to Information Security

Prof. Dilip H. Ayyar

Department of Computer Science and Engineering

Indian Institute of Technology, Madras

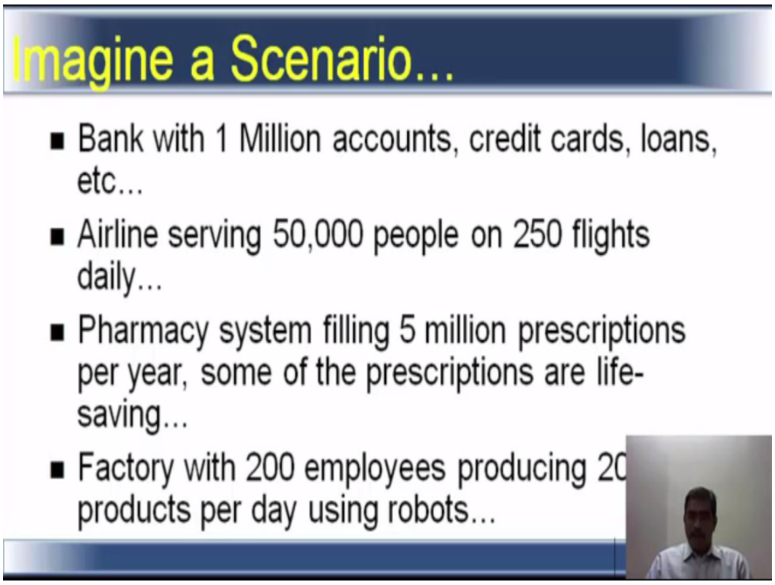
Lecture – 37

(Refer Time Slide: 00:11)

BCP / DRP

Let us now see, what is a BCP and DRP.

(Refer Time Slide: 00:16)

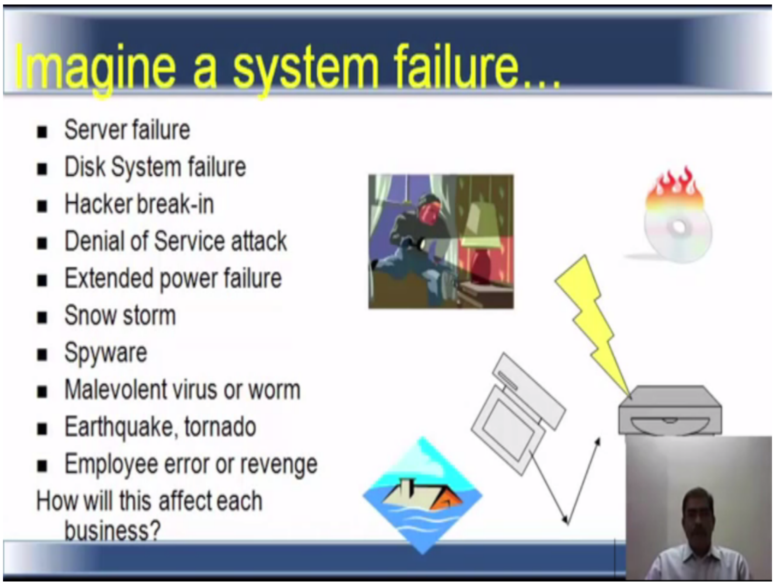


Imagine a Scenario…

- Bank with 1 Million accounts, credit cards, loans, etc…
- Airline serving 50,000 people on 250 flights daily…
- Pharmacy system filling 5 million prescriptions per year, some of the prescriptions are life-saving…
- Factory with 200 employees producing 20 products per day using robots…

Imagine a scenario, where there is a bank with 1 million accounts, there are credit cards, loans, fixed deposits, or you take the example of an airline, serving which is in 50,000 people, on 250 flights every day. Or a pharmacy system filing 5 million prescriptions per year, some of the prescriptions are life saving or a factory, with 200 employees producing 2,00,000 products per day using the robots.

(Refer Time Slide: 00:52)



Imagine a system failure…

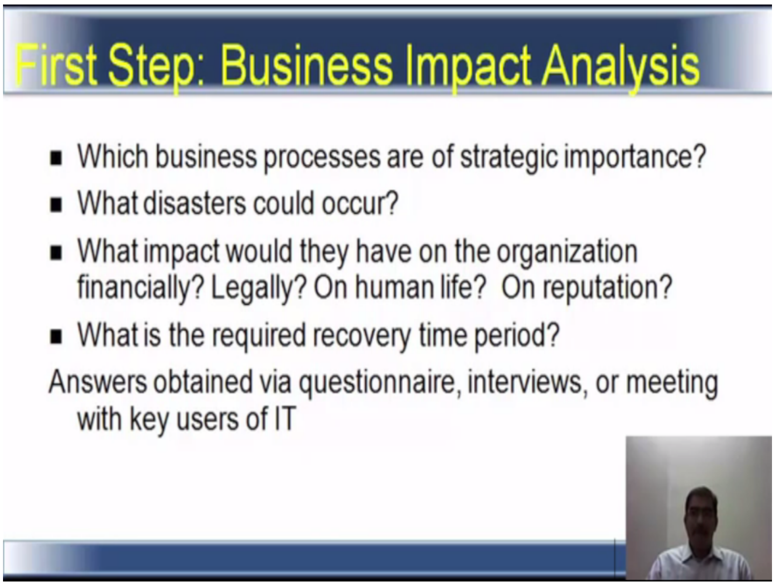
- Server failure
- Disk System failure
- Hacker break-in
- Denial of Service attack
- Extended power failure
- Snow storm
- Spyware
- Malevolent virus or worm
- Earthquake, tornado
- Employee error or revenge

How will this affect each business?

Now, with that scenario, imagine a system failure, be it server failure, or a hard disk failure or break in by hacker, denial of service attack, extended power failure, snow storm, or a cyclone, or spyware gets into the system, or virus, or a worm, natural disaster occurring like earthquake, or a tornado, or a disgruntled employee or damage done for revenge.

How will do these factors affects each of business, which we discussed earlier about it, now, different companies will react in different ways to the problems. A bank may want to bring down the network as soon as possible, if the intruder penetrates the network. A pharmacy, may want to leave there network as much as possible, but they do want to double check the integrity, or deicide to bring down a partial network.

(Refer Time Slide: 01:58)



First Step: Business Impact Analysis

- Which business processes are of strategic importance?
- What disasters could occur?
- What impact would they have on the organization financially? Legally? On human life? On reputation?
- What is the required recovery time period?

Answers obtained via questionnaire, interviews, or meeting with key users of IT

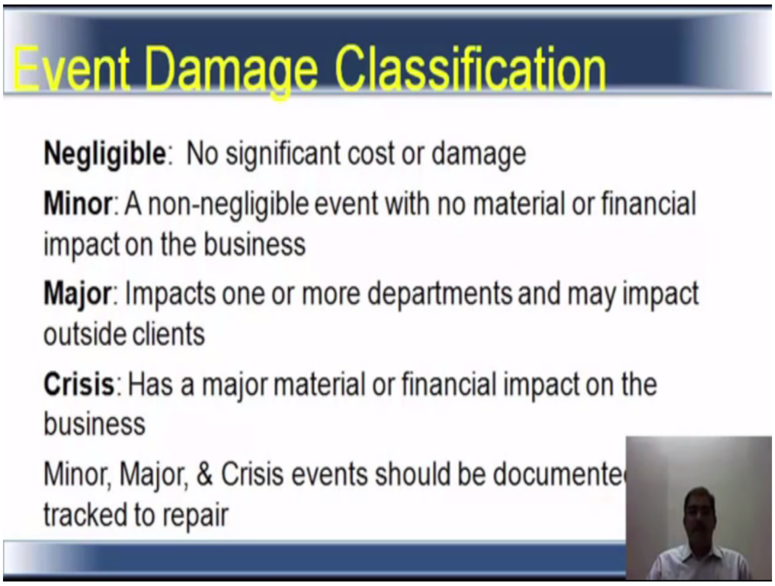
Business continuity plan is effectively bringing back your business, after a incident occurs. The incident is any event, which has an undesirable effect on the organisation continuity. Now, there are several faces in a BCP process, the first step is the business impact analysis, what does it address which business processes, are of strategic importance.

So, which services can go down, and which services have to stay alive, for the continuity of operation. What disasters could occur, a business impact analysis would also specify what disasters could occur, what are the ways which it could occur. So, all possible scenarios as we discus in the previous slides should be addressed in the business impact analysis.

Now, what impact would they have on organisation, financially, legally, on human life that on personnel within, and the customers, on the repetition. And what is the required recovery time period, how fast, we should bring back the operation, whether it is 2 hours, 4 fours, whether it should come back in 20 minutes. All this things will be specified, in the business impact analysis.

Now, there are several ways to get this information, it can be via interview, it can be via questionnaire, it can be through observation, review of documentation, there are several ways of conducting the business impact analysis.

(Refer Time Slide: 03:46)



Event Damage Classification

Negligible: No significant cost or damage

Minor: A non-negligible event with no material or financial impact on the business

Major: Impacts one or more departments and may impact outside clients

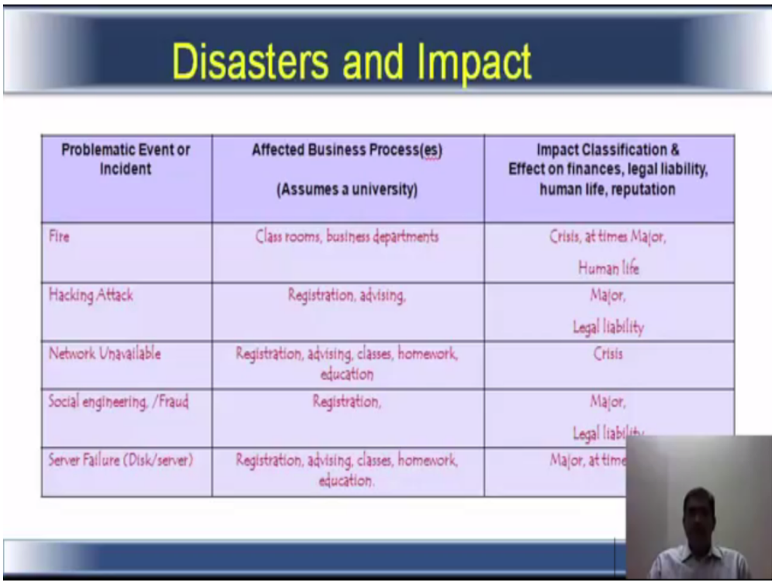
Crisis: Has a major material or financial impact on the business

Minor, Major, & Crisis events should be documente tracked to repair

When we talk about business assumption, we also have to classify the assets. Asset classification as a very important step, where the value of the assets is arrived at, and the damage potential for that particular asset, and a general trend for a classification of event is negligible, which means there is no significant posture damage. It could be a very simple issue, which can be recovered with a no time. It could be a minor event which is non negligible event with no material, or financial impact on the business.

Major where the incident impact one or more department, and may impact outside clients as well, and then the final one is the crisis which has a major material of financial impact on the business. Now, all these things that is your minor, major, crisis should be documented track to resolution, or repair that means to say that if an event occurs, you have document you will have to specify, what actions are taken to rectify that error, or to bring back the business normal size. So, this should be tracked.

(Refer Time Slide: 05:08)



Disasters and Impact

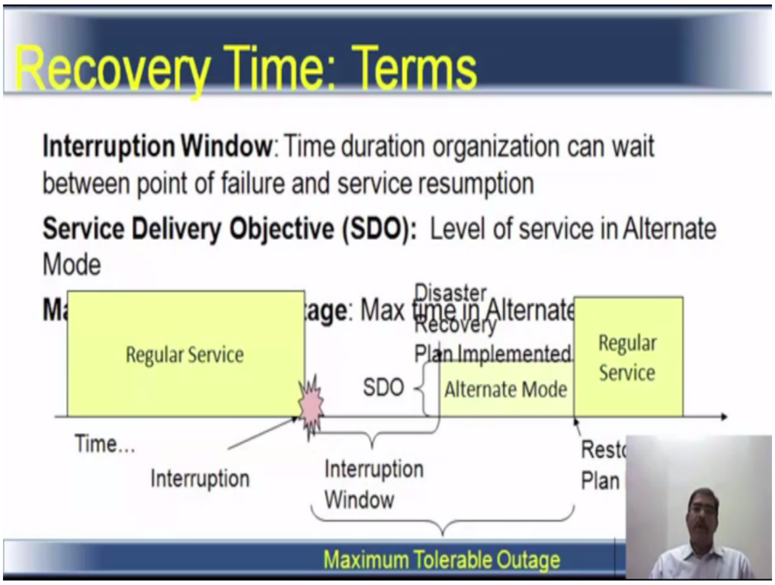
Problematic Event or Incident	Affected Business Process(es) (Assumes a university)	Impact Classification & Effect on finances, legal liability, human life, reputation
Fire	Class rooms, business departments	Crisis, at times Major, Human life
Hacking Attack	Registration, advising,	Major, Legal liability
Network Unavailable	Registration, advising, classes, homework, education	Crisis
Social engineering, /Fraud	Registration,	Major, Legal liabi
Server Failure (Disk/server)	Registration, advising, classes, homework, education.	Major, at time

Let us see a scenario, disasters and impact, where the problematic event or incident is o classified, what business processes are affected, and the classification of the impact, effect on the finance, legal library, and the effect on human life and on the repetition of the business. Now, this example has been done assuming that, the organisational is a university. So, let us take as a first example, if the incident is the fire, then the affected business processes are the class rooms, and the business departments.

And what is the impact? It is crisis, that means it is ranked highest, at times major. And what could be the damaging factor, there could be damaging, a human life also. Then second one is hacking attack, in case of hack occurs, then your registration and advising or conselling is affected, the impact is classified as a major, that could be legal implications, if such a thing occurs.

If the network is unavailable then your registration is affected, consoling is affected, the classes are affected, home work and education is affected. And it is classified as highest level crisis. If a social engineering or a fraud occurs, it affects registration. It is classified as major, there could be legal implications of that. If it is sever or hard disk failure, then registration gets affected, conselling gets affected, classes, home work and education get affected, and major at times, and crisis other times, meaning at the time of the registration or when a home work is due to be given, or if a class is to be taken, it could be crisis.

(Refer Time Slide: 07:12)



Recovery Time: Terms

Interruption Window: Time duration organization can wait between point of failure and service resumption

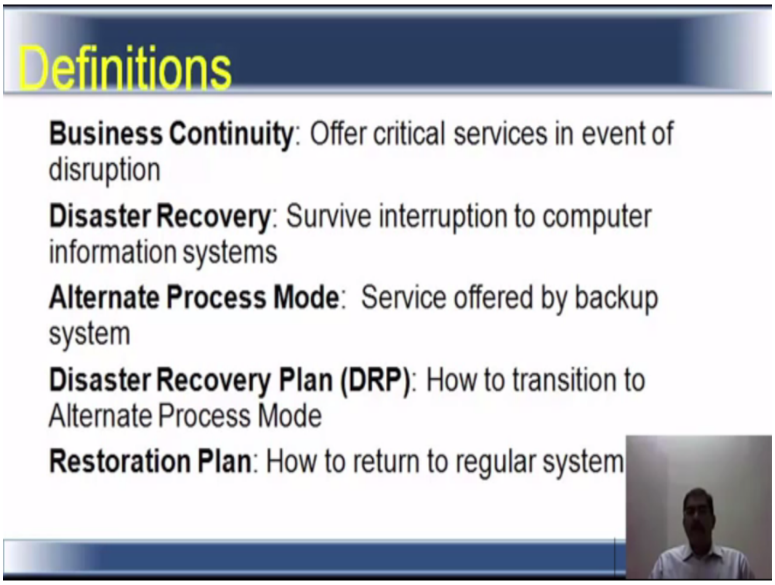
Service Delivery Objective (SDO): Level of service in Alternate Mode

Ma **age**: Max time in Alternate

How you define recovery time? There is something called as interruption window that is the time duration that the organisation can wait, between the point of failure, and service resolution. For example, you can say that a particular process in my organisation, if it goes down which is critical to the organisation, should be recovered within 30 minutes from the time of failure. So, that is the interruption window.

What is the service delivery objective, level of service in alternate mode, in the sense in case if we are not able to do it through the computer, do you have any process where you can actually process with manual, so that the service delivery objective is met. These are the things, that from part of recovery time. One thing you have to remember is the alternate mode is not a full service mode, your service will continue, but at a degraded base. You have to, because the cost of providing service in an alternate mode also involves the lot of time, effort, money and people. Hence, we will have to understand that alternate mode in not always, a full service mode.

(Refer Time Slide: 08:35)



Definitions

Business Continuity: Offer critical services in event of disruption

Disaster Recovery: Survive interruption to computer information systems

Alternate Process Mode: Service offered by backup system

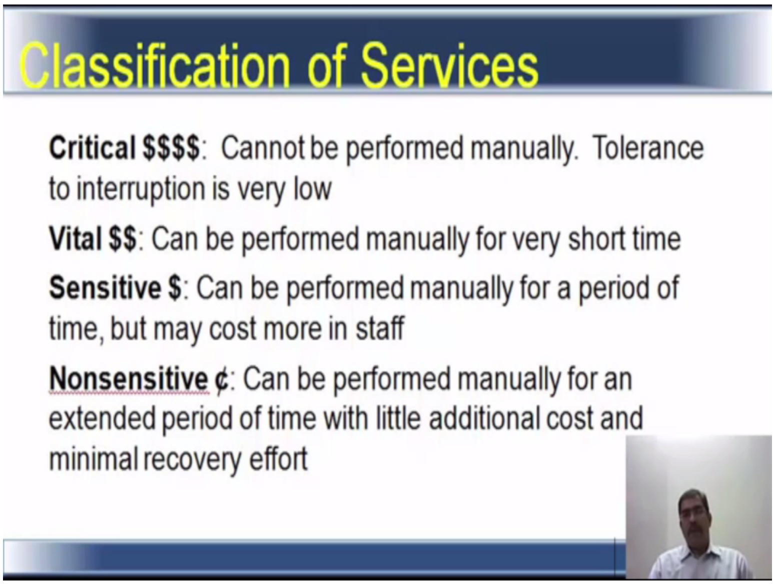
Disaster Recovery Plan (DRP): How to transition to Alternate Process Mode

Restoration Plan: How to return to regular system

Let us look at some definition, business continuity means offer critical service in event of disruption. Disruption can mean incident, whether malicious are not. Human failures also can be classified as incidents. Disaster recovery is survive interruption, to computer information systems. So, basically your BCP is a large document, within which your IP processing the address, which is called a disaster recovery plan.

Then, there is an alternative process mode, which is service offered by backup system. It can be, at an outside or a near site of location, it can be at different sites by an external vendor like a hot site, warm site, cold site, reciprocal agreement. We will look into all those. Then disaster recovery plan is how to transition, to do alternate process mode. For a disaster recovery plan fixing, when your incident actually happens, and when your BCP actually is involved. And then the restoration plan.

(Refer Time Slide: 09:53)



Classification of Services

Critical $$$$: Cannot be performed manually. Tolerance to interruption is very low

Vital $$: Can be performed manually for very short time

Sensitive $: Can be performed manually for a period of time, but may cost more in staff

Nonsensitive ¢: Can be performed manually for an extended period of time with little additional cost and minimal recovery effort

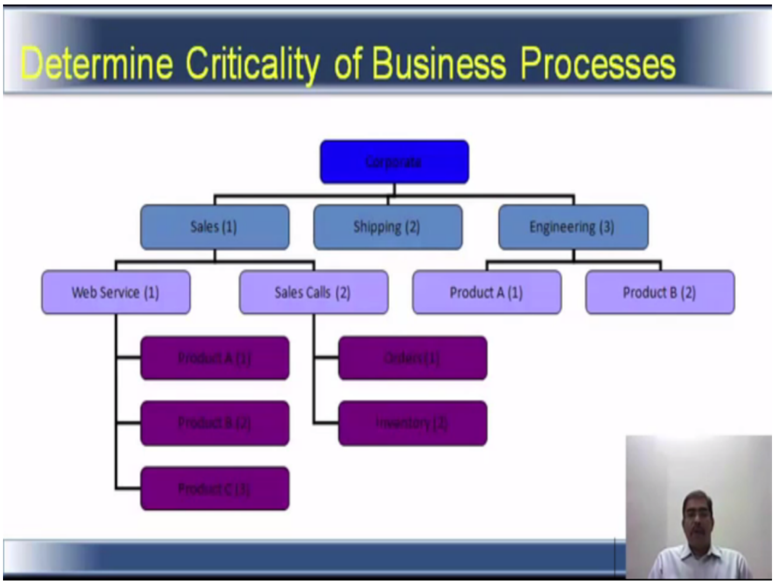
How to return to regular system, that is how to resume normal operation after a event occurs or an incident occurs, how you classify the services. Critical, it cannot be performed manually, tolerance to interrupt is very low. There may be some process, which cannot be performed manually. So, the tolerance is also very low, you have to recover the operations very fast. Take the example of ERP system, you enter a row material to one place, it gets reflected in different portions of ERP.

It may not be manual possible to recreate, or recreate that particular according to different places, once at organisation is fully into an ERP mode. Then vital problem, it can be performed manually for very short time. For example, if it is a product service or, product sales company, you can still manage to get manual bills, and giving to the customer, it will be sensitive. It can perform manually for a period of time, but may cost more in staff.

Assume that, HR system does down, you have hundred employees. You need to pay their salary. You can perform manually calculated manually for period of time. But, you need additional man power to do that, but then this is not always applicable say to an organisation with 5000 employees. Then it takes lot of effort, lot of time, and may not finish on time.

Then you have non sensitive, which can be performed manually for extended period of time, with little additional cost of minimal recovery of, there may be some processes, which do not require the computer, or which you can do within the time of invoking of BCP. So, these can be performed manually for extended period of time with little or no additional cost, and minimal recovery effort.

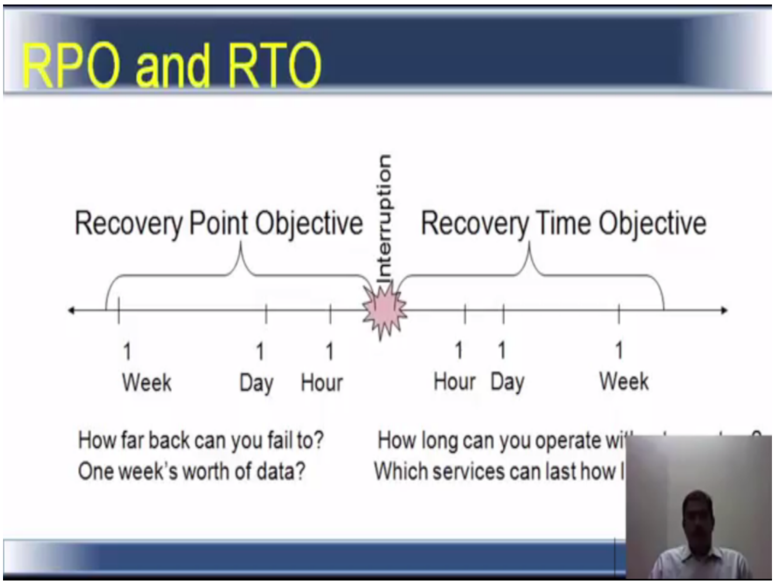
(Refer Time Slide: 11:52)



Determine Criticality of Business Processes

How do you determine the criticality of business processes? Take this pictorial for example, there is a corporate structure, here sales function we designed that sales function is very critical, so sales is number one. If we do not have sales, we do not ship or we do not manufacture. Engineers can work at home on their projects, so the criticality of business process, should be determine before you actually assign values to that. Also it is always a good idea and upper management, or top management or senior management. However you call it should have or should play an active role in determining, the criticality of business process.

(Refer Time Slide: 12:36)



RPO and RTO

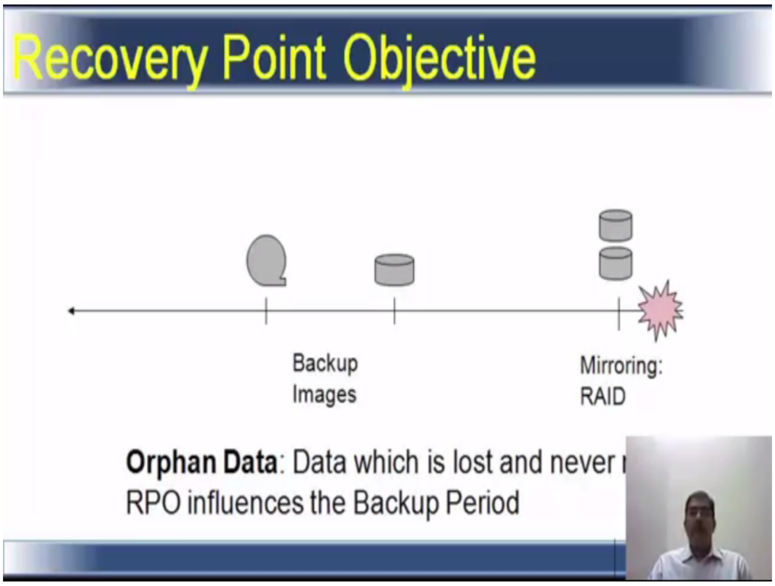
How far back can you fail to?
One week's worth of data?

How long can you operate wi
Which services can last how l

There are two terminologies here, RPO and RTO, RPO is recovery point objective and RTO is recovery time objective. What RPO determines is, how far can you fail, is it one week's worth of data, and recovery time objective is how long can you operate, without a system, and which services can last for how long. So, these basically are the two factors that you will have to determine one is the RPO and other is the RTO.

Now, if you have one week's work of data, is it sufficient to recover, or do you need a back up of say, the latest one which is taken every night, or in some cases the RPO may be very short. Because, there is an online mirroring of data which happens, where all depends on the business that the organisation is into, and how valuable is continuity of source to the organisation.

(Refer Time Slide: 13:46)



Recovery Point Objective

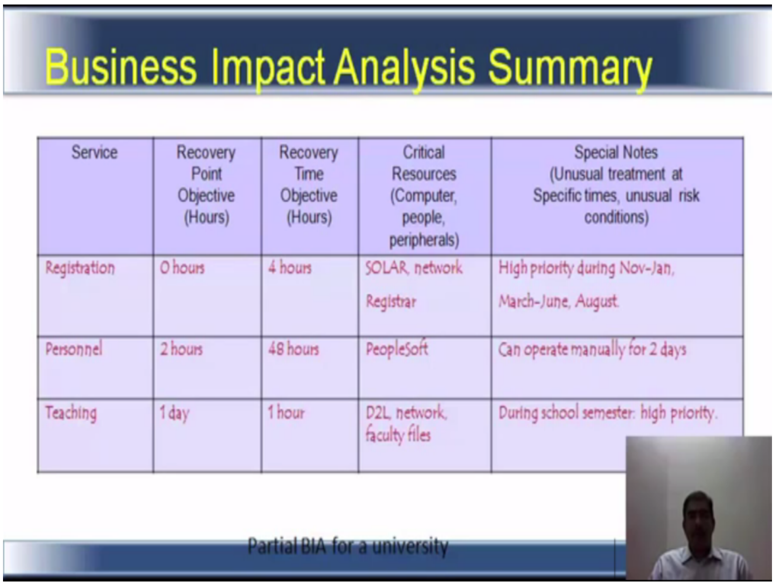
Orphan Data: Data which is lost and never r

RPO influences the Backup Period

When we look at RPO, you need to have backups. So, there is something called orphan data. Orphan data is a data which is lost, and never recovered. And the recovery point objective actually influences the backup period, like I said, the most critical your data is the more enfaces some back up it. Could be as costly as an online marine system, or every hour back up is taken, every evening back up is taken, then every week back up is taken.

So, it all depends on the criticality of business processes. Also, we have mentioned here also RAID. So, the RAID is redundant array of inexpensive disk. This is for internal, to protect against your internal disk failure. And, also to have more reliability on the fact that, once you configure yourself on a rate system addresses, your rate system in the event of the disaster happening or in the event of the disk failure, you still will be able to recover data and continue with the operations.

(Refer Time Slide: 15:00)



Business Impact Analysis Summary

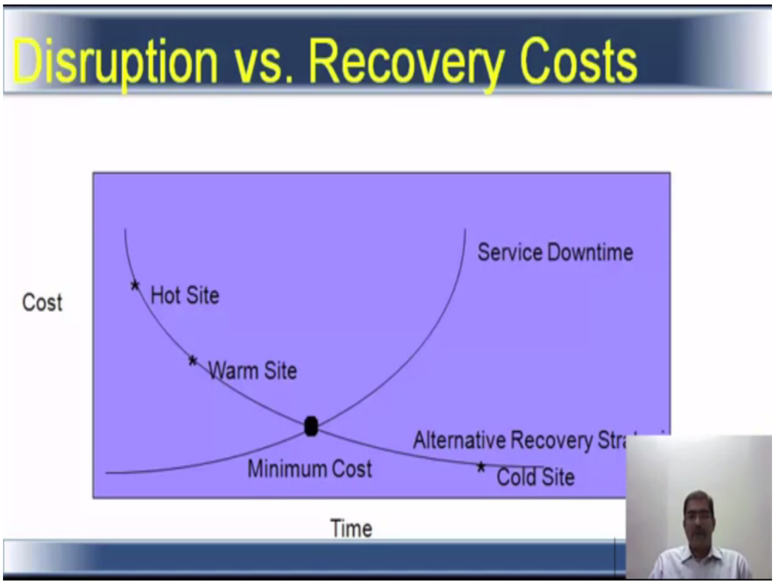
Service	Recovery Point Objective (Hours)	Recovery Time Objective (Hours)	Critical Resources (Computer, people, peripherals)	Special Notes (Unusual treatment at Specific times, unusual risk conditions)
Registration	0 hours	4 hours	SOLAR, network Registrar	High priority during Nov-Jan, March-June, August
Personnel	2 hours	48 hours	PeopleSoft	Can operate manually for 2 days
Teaching	1 day	1 hour	D2L, network, faculty files	During school semester: high priority.

Partial BIA for a university

So, now we add a couple of columns to this slide we saw earlier, this services registration, here we are added the RPO and the RTO for registration, the recovery point of objective is 0 hours, the time objective 4 hours. Critical resources, people process and technology, you have solar based battery backup, network redundancy, registrar is important aspect here, and special notes, unusual treatment of specific time, unusual expenditure, its high priority during November and January.

That is where maximum registration are done, March to June, and in august. So similarly, for personnel, 2 hours is RPO, 48 hours is RTO. People saw, which is in an ERP package he is a critical resource, and without that ERP also, you can operate manually for 2 days. Teaching, your RPO is 1 day your RTO is 1 hour. And you have your d2l link network, your faculty files as the critical resources, then special notes, you have during school semester. It is a high priority, meaning during the school period or college period it is a high priority. This is how partial BIA, looks like for an university.

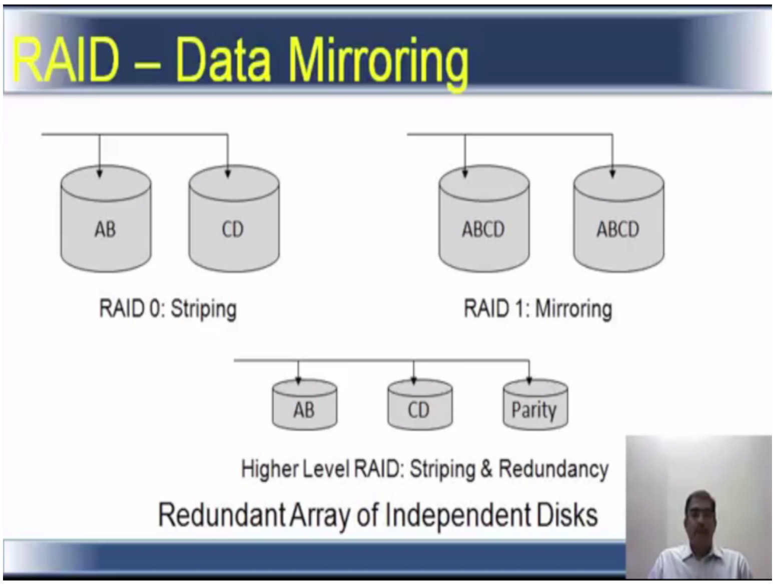
(Refer Time Slide: 16:35)



Disruption vs. Recovery Costs

When you see description versus a recovery costs, you have several notes here, like hot side, warm side service down period, alternative service cold site. So, this is a curve showing the cost having a system down, and the other curve shows the cost of bringing an alternative system up quickly. So, the least cost is, the cross point of this two curves to brief into the BCP, DRP will give you an idea of, what a business continuity plan is. What is a business impact analysis, what is RPO and RTO, what are the methods you can use, what is the curve your minimum cost curve. Let us take a look at, what is the RAID in simple terms and what is the high availability solution avail in the next.

(Refer Time Slide: 17:31)



RAID – Data Mirroring

Redundant Array of Independent Disks

RAID is basically redundant array or random array of independent disks. Now, there are several levels of it, RAID 0 striping, 1 is mirroring then the other RAID 2,3, 4, 5, 6, 7, 10, 10 is a combination of 1 and 0. So, RAID 1 and above uses redundancy offering in survival, if a single disk fails. Let us go back little bit on history of a RAID. There was a time, and hard disk had less capacity, and more expensive.

Raid was created to combine multiple, lets an expensive RAID into a single higher capacity or a faster volume. On top of that, it was designed to facilitate redundancy. So, that is usually called as fault tolerance, or sale over protection. So that the array and its data remain usable even when a drive fails. You will often here about 1 disk, or 2 disk redundancy. It refers to the number of drives that can fail while array remains liable or operational.

Redundancy is very important for small businesses. As for drive failures, can happen for there is nothing that can prevent that. RAIDS data redundancy offer, no protection against data loss. So, you all need to understand that raids are not to protect against data loss due to malware, or else natural disaster. And, it is not a substitute for backuppractises. But, it will provide, failsafe protection mechanism against hardware failures.

RAID has many levels, or methods by which the drives are team together. A common person refers to levels by numbers. The three most common levels, what are available in market a RAID 0, RAID 1, RAID 5, but you will also come across numerous other options like level 6 and 10, 6 is 5 plus 1. So, it is just a bunch of disks, and Microsoft virtual disk array, as well as abstracted RAID implementation, such as a drobo, beyond raid, netgear x raid , sinal d shr etc.

So, there are so many things, but let us see what are the common RAID modes, RAID 0 is faster performance, and it distributes data across multiple RAIDS. For example, block A goes to an end from drive 1, block B goes to an end from drive 2, which permits increased read, and write beats. These approach is sometimes called as tribic, and other modes of RAID also employ these techniques. Raid 1 reads or raids, and reads the data to the pair of drives. It will also refer to a mirroring.

The drives are equal partners, should either fails you can continue to work with the good one until you can replace the bad one. Raid 1 is the simplest, and the easiest method to create a fail over disk storage. However, it cost you 50 percent of the total available drive capacity. For example, if you take 2 1 tb drives in a mirrored array, we will give only 1 TB of usable disk, not 2 tb. Then there is something called RAID 5, RAID 5 offers both speed and data redundancy.

Raid 5 writes disk to, and read from multiple disks. It distributes a parity data across all disks in the RAID. Parity data is a smaller amount of data, which is drive mathematically from a larger set, that can accurately describe, that larger amount of data. So, it serves to restoring. Since, parity information is distributed across all drive. Any drive can fail without causing the entire array to fail.

But, RAID 5 uses one third of available disk capacity for parity information, and requires a minimum of 3 disks to implement. Since, data is read from multiple disks, performance can improve under RAID 5, but some users report that RAID 5 slows performance greatly, when it is processing, the multiple reads on the server situation. JBAR is a short name for a just a bunch of disks, it is actually not RAID.

But, it is often available as an option and multi disks storage boxes that offers RAID. Jbar offers, no speed increase or redundancy. But, it simply concatenates a group disks into a single volume. Then, there is drive extent of a Microsoft, but that, the Microsoft is abandoned this technology, which was formerly employed on Match boxes running Microsoft windows home server. So, these are the basic RAID methods, that are available and the most common one.