Introduction to Information Security

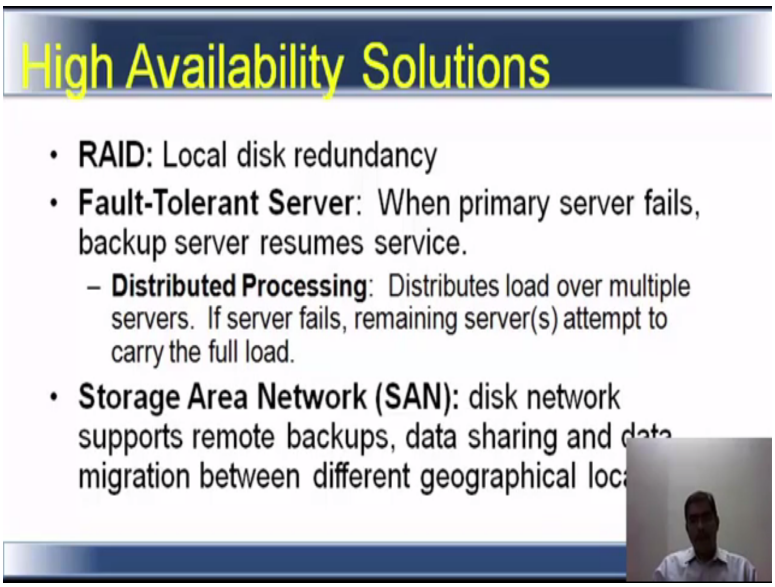
Prof. Dilip H. Ayyar

Department of Computer Science and Engineering

Indian Institute of Technology, Madras

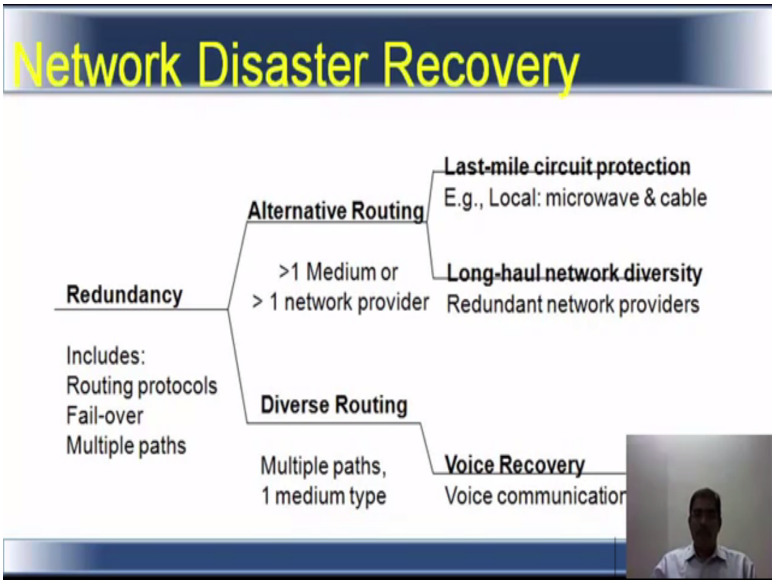
Lecture - 38

(Refer Time Slide: 00:10)



Now, raid provides local disk redundancy. It is a high availability solution. Fault tolerant server so, when the primary server fails, backup server resumes service. The feature of this is distributed processing. It distributes load over multiple servers, if server fails remaining servers attempt to carry the full load, a sort of like how the cloud technologies works today. San or storage area network so, disk network that supports remote backups, data sharing, and data migration between different geographical locations.

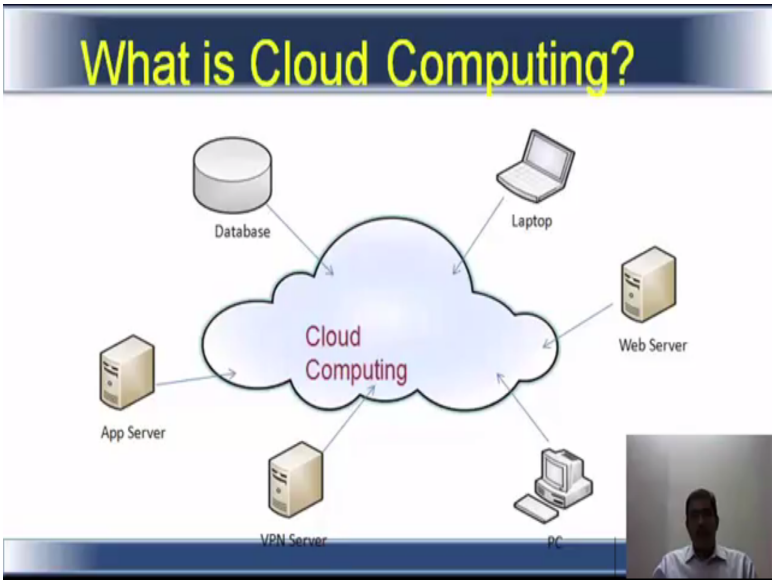
(Refer Time Slide: 00:48)



After a brief about raid, let us come back to network disaster recovery, which is again we go back to the bcp, drp process. Now, this is a graphical or pictorial representation of how a network disaster recovery happens. There are several components, one is the redundancy, what it includes is routing protocols, fail-over, multiple paths. So, with redundancy, if one path fails, another path can take over.

Then there is alternate routing or diverse routing, diverse routing means one provider, but multiple route. Alternate routing means multiple network providers, or multiple mediums, mediums like fiber or cable or radio. Then last mile protection, if everything else fails, you have microwave or cable, you have long haul network diversity, which are the redundant network service providers. Then voice recovery, voice communication backup. So, with a little bit of raid and network disaster recovery, we conclude this and go to cloud computing, where we will discuss about different modes of vigile.

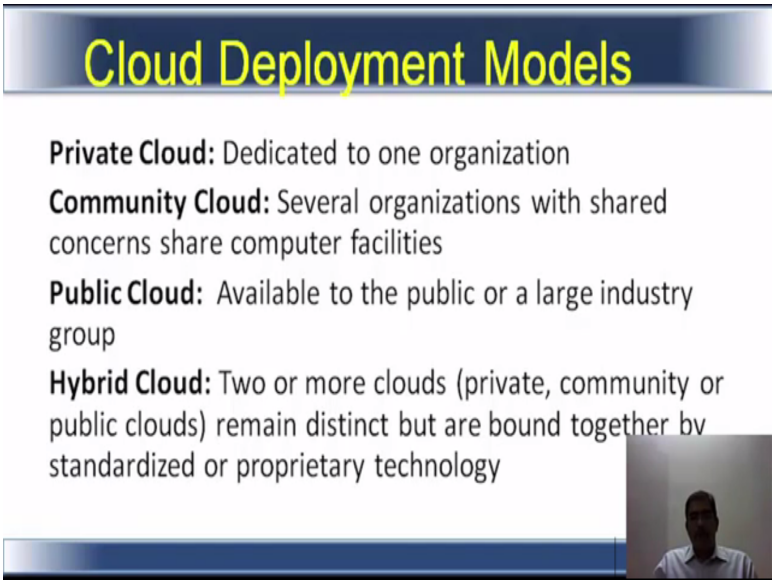
(Refer Time Slide: 02:05)



We have seen, what is, cloud computing in doctor Kamakoti's class. But, just to refresh your memory , let us see what, is cloud computing. Cloud is nothing, computing is nothing but a shared pool of configurable computing resources, what are the computing resources, servers, application, databases, the services that are on the computers, the network, these are all the shared pool of configurable computing resources.

Why it is called, because it can be rapidly customized, and released with minimal management effort, or minimal effort from the part of service provider. So, any user within the network is allowed to the access the shared configurable resources, after providing sufficient authentication. Once the authentication is approved, or recognized by the system, the user is able to access the customized resources. Here, that means the resources that are allocated to him, or the resources he needs to work on. Basically, you can say need to know, need to do basis.

(Refer Time Slide: 03:20)



We have different cloud deployment models, like a private cloud which is dedicated to one organization, or a community cloud where the several organizations where share the common facilities. A public cloud which is available to the public or a large industry group, hybrid cloud two or more clouds, it can be a combination of private community or public. It remains distinct, but are bound together by standardized or proprietary technology.

(Refer Time Slide: 00:48)

There are major security concerns in cloud also, one is multi tendency, and your application is on same server with other organizations. So, you need segmentation, you need to be isolated, you need a policy with governs of service provider, and for the access. Then the physical location of the cloud service provider, it is what we have server itself in which

county will the data reside, what regulations affect the data. PProper SLA should be there. SLA should define performance, the security policy, availability, back up, location, compliance issues, audit issues or right to audit clause. Your coverage, total security is your portion, plus your service provider portion. So, the responsibility varies actually from infrastructure as a service, versus platform as a service versus software as a service. You can transfer the security responsibility to the vendor, but not the accountability. Ultimately the data or the processing is done by you, and your employees.

(Refer Time Slide: 05:02)

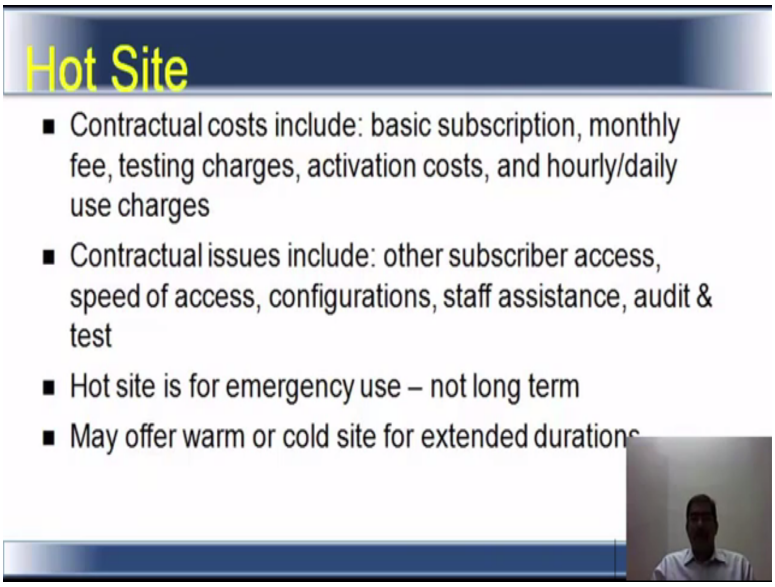
Now, let us see alternative recovery strategies. Again, we come back to BCP, so we saw what are in brief we saw what is hot site, warm site, cold site, redundant information processing facility, reciprocal agreement, mobile site. Let us see that in detail, now hot site is a fully configured, ready to operate facility, that means it can be ready within a matter of hours. Warm site is ready to operate within days, it will generally not have power, or it will have low power, and it will contain disks, networks, peripherals etc.

Cold site will be ready to operate within weeks. It will just contain a basic electrical wiring, air conditioning, flooring etc. No computers, it has just the bare facilities. Duplicate or redundant information processing facility, it is also called as standby hot site, we can say the backup server is within the organization itself. Reciprocal agreement, reciprocal agreement with another organization or another division at another location, then mobile site it is fully or

partially configured trailer that comes to your site with microwave or satellite communication.

I am sure that many of you have seen, in India in certain banks, where mobile ATM's are there with satellite link or microwave link, it go to different area, within the city where users can access the ATM's, and do some transactions with the kiosk available within the mobile agents. So, that is a mobile site.

(Refer Time Slide: 06:52)

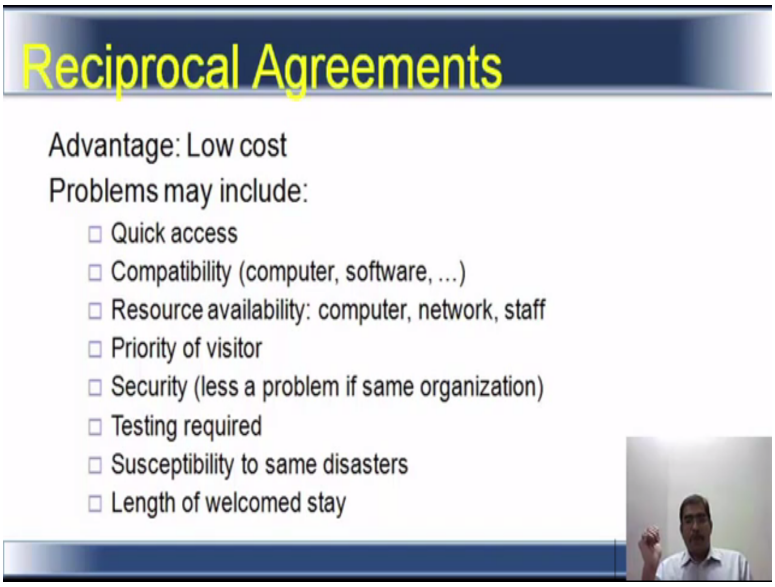


What is a hot site, you had seen them, but there are contractual costs, which go around the hot site. That will be a basic subscription charge, or monthly fee, testing charge, activation charge, and hourly or daily service usage charge. So, there are different modes of having the contractual application, or contractual agreement with the vendor. Contractual issues will include, other subscriber access, meaning in the event of a natural disaster, whether the vendor give the facility to another subscriber also.

Does it affect our operation, then at what speed of access he can give, how fast he can give the access the configurations, how fast can it be done. What staff assistance will be available, staff assistance will be available, whether the organization can audit, and test the vendor's facility. And then, basically a hot site is very expensive mode of alternate processing. It should be used only in emergency, and not as a long term prospect.

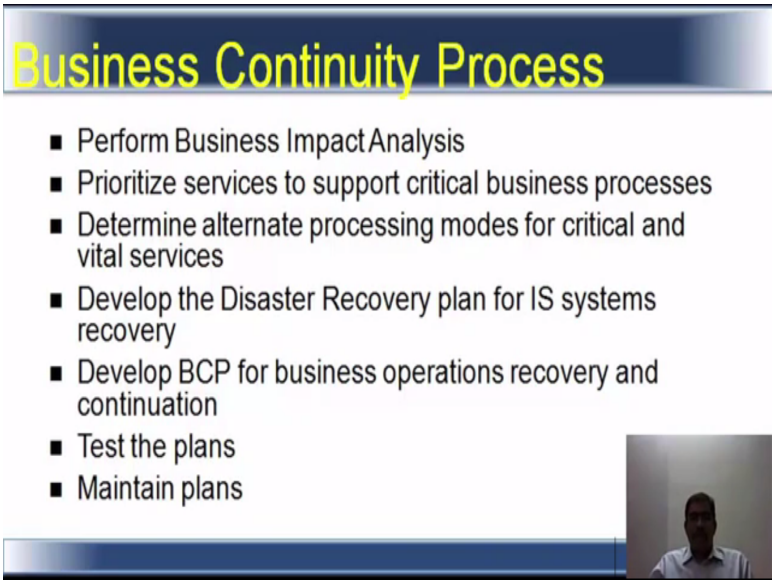
Now, if the organization feels that the recovery is going to take longer than expected, then they may choose warm site or cold site for extended duration, or vendor may provide, or offer warm or cold site for extended duration.

(Refer Time Slide: 08:25)



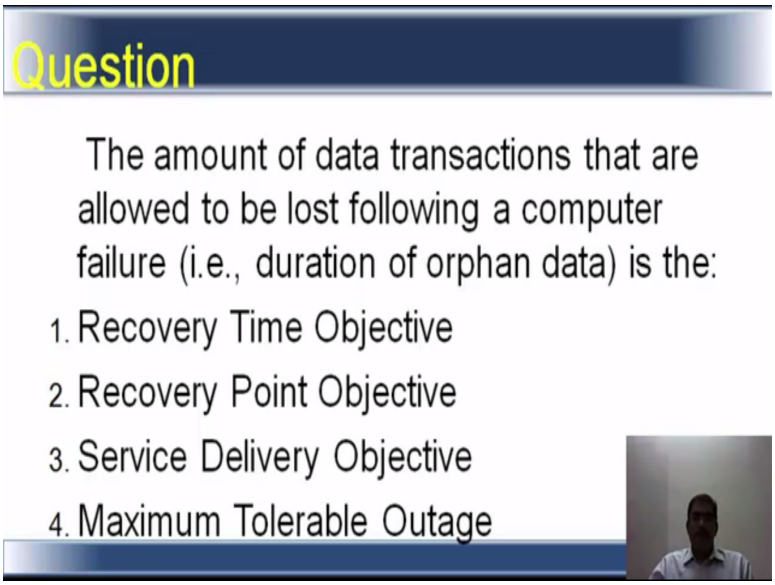
Reciprocal agreements, the basic advantage is low cost. That is you collaborate or corroborate with another organization, to perform your alternate processing along with them. But, there may be problems like, quick access, then compatibility of computer, the software, the hardware, the resource availability, availability of computer itself, availability of adequate network, availability of staff, priority of the visitor which visitor gets precedence, whether it is the subscriber who is going to do work, whether, it is company that is hosting a company, or your visitors. Security is less of a problem, if it is the same organization, because we know what to expect. Then it has to be tested, we see the syncability and adequacy. But, then our reciprocal site also is susceptible to the same disasters, and you cannot stay there forever. So, the length of welcome stay is another issue. Now, we have looked at various things.

(Refer Time Slide: 09:42)



Now, let us see what is the bc process is, the business continuity process, you have seen what a bia is. So, first we do a business impact analysis, then we prioritize services to support critical business processes. We determine, alternate processing mode for critical and vital services. We develop the disaster recovery plan, for information systems recovery. We develop a bcp for business operations continuity, and recovery. Then we have to test the plans, maintain the plans to reflect the changes, which have happened in the organization, since the document was made.

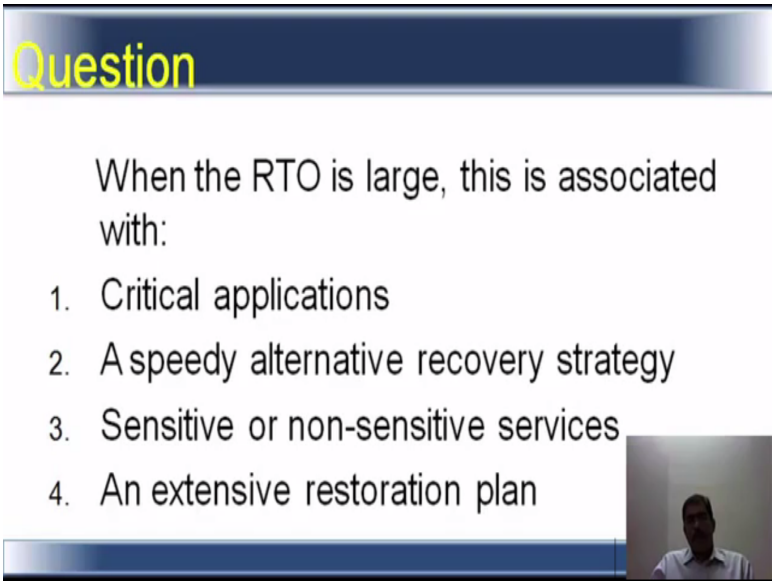
(Refer Time Slide: 10:42)



Let us look at some simple questions on b c p. now, the first question is, amount of data transactions that are allowed to be lost, following a computer failure, that is duration of

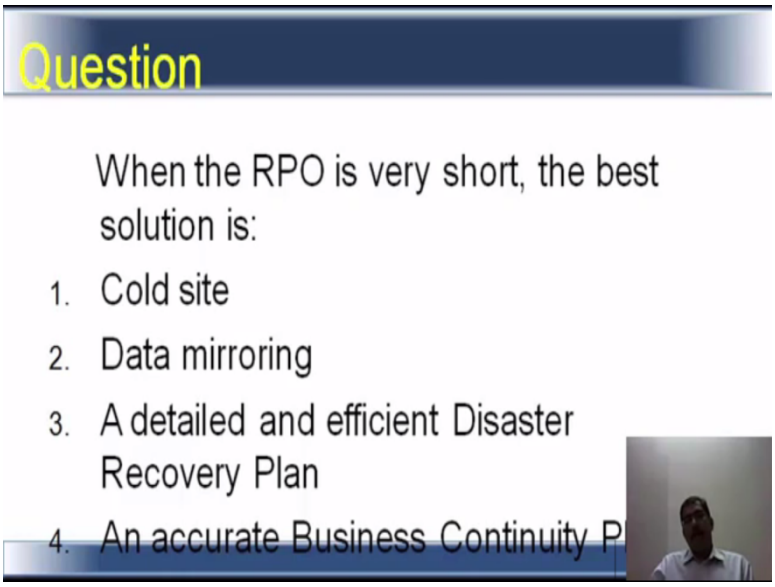
orphan data is, 1 the rto, 2 rpo, 3 service delivery objective, 4 maximum tolerable outage. Now, the answer for this is 2.

(Refer Time Slide: 10:54)



Next question is, when the r t o is large, this is associated with, 1 critical applications, 2 speedy alternative recovery strategy, 3 sensitive or non-sensitive services and 4 extensive restoration plan. The answer for this is 3, because large rto means, the application can run manually, with little problem for an extended period of time. This is associated with the services classified as sensitive or non-sensitive.

(Refer Time Slide: 11:30)

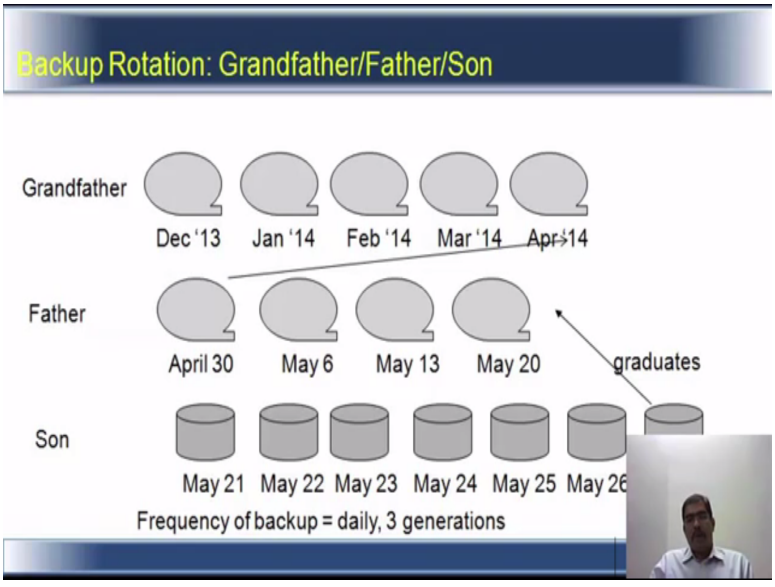


The third question, when the r p o is very short, the best solution is, 1 a cold site, 2 data mirroring, 3 detailed and efficient disaster recovery plan, 4 an accurate bcp. The answer is 2 data mirroring, because rpo requires recovery of data, that is gathered in the past immediately, therefore the correct answer is data mirroring here.

(Refer Time Slide: 12:01)

Or using the redundant disks raid, now, let us take a look at data storage protection. We have already seen, what raid is, so you have fair bit of idea how raid operates.

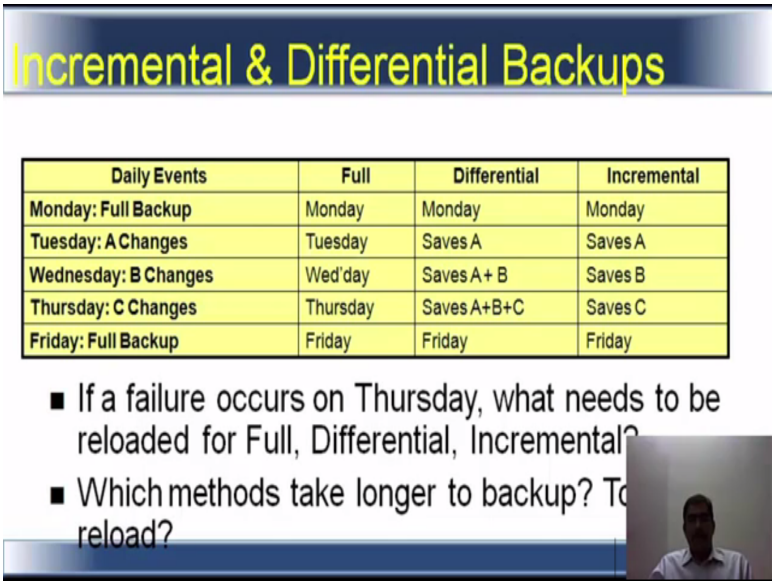
(Refer Time Slide: 12:18)



Let us see the requirements of data storage protection, or backup storage. If you look at the slide here, the backup rotation is called grandfather, father and son. If you see grandfather, it is monthly, December 13, January 14, February 14 etc. The father is April 13, May 16, May 13, and May 20th. So, father has a gap of seven days in the back up. Grandfather has monthly, father is weekly. The son is May 21, may 22, May 23.

So, it is a daily backup. The son, the disk rotates in the son back up, the disk rotates 7 times, or 7 disks are continuously rotating. In the father mode of backup, 4 to 5 tapes are rotated with the oldest being overlaid, overlaid means over written. Grandfather is monthly so 12 or 24 tapes, can maintain a monthly history for 1 or 2 years again, depending upon the organization's requirement.

(Refer Time Slide: 13:20)



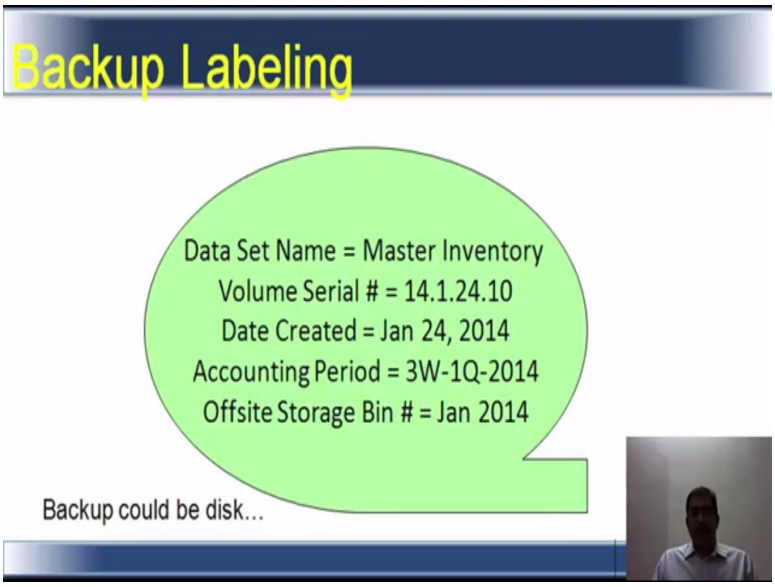
Then there is incremental and differential backup. If a failure occurs on Thursday, what needs to be reloaded for full differential and incremental backup, which methods take longer to backup, or which methods take longer to reload, all this can be addressed by this. Now, if you take the picture, above the daily events, Monday is a full backup, Tuesday a changes, Wednesday b changes, Thursday c changes, Friday there is a full back up.

So, again if you see on the right hand side, the 3 columns, Monday is a full backup and there is a differential backup, and incremental backup happening on Monday, on Tuesday. It saves a incremental, also saves a Wednesday, b changes, so in differential back up it save a plus b

Thursday, c changes so in differential back up a plus b plus c changes, and Friday of course, full back up happens.

So, you basically need to understand the difference between incremental and differential back up. Now, in incremental backup, you have seen it saves a, it saves b, it saves c in differential back up. It save a plus b, and then it saves a plus b, plus c, there is no use of taking a backup, if proper labeling is not done.

(Refer Time Slide: 14:45)



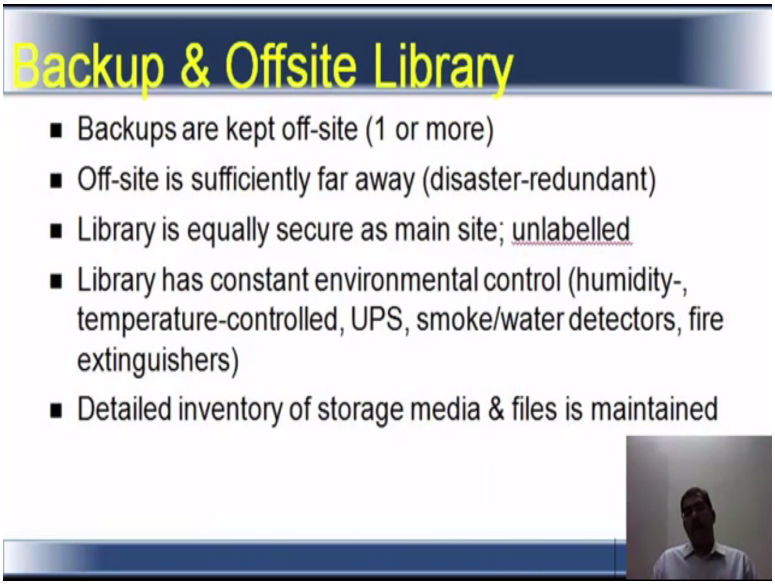
So, a sample backup labeling is shown here, a backup can be a disk or tape or dvd, depending upon the requirements. It should at least have a data set name, which may be the master inventory. It should have a serial number, volume serial number, it could be a date, or disk number when it was created, and what is the accounting period, so you can always say 1415.

So, here it is third week first quarter of 2014, then offsite storage in January 2014. So, it should have a proper labeling system, to identify what was taken. There should also be proper restoration testing done, though many organizations take back up on a daily basis. But, they fail to check, what is whether any data has been written to the tape. So, the backup testing is not done, that is a very important and crucial aspect.

So, restoration testing requires time, and it needs additional resources in terms of computer, it needs additional manpower, but it has to be done. What is the use, if the data is not written, not written on a tape or your disk or your san, and at the time of an incident, when you want

to recover it, you find that there is nothing there. So, the backup, all these process have to be done, plus the restoration testing have to be done diligently.

(Refer Time Slide: 16:20)



It is always a good practice, to keep one copy of the backup off site, better if it one or more and the offsite location should be sufficiently far away. That means, the location should not be prone to the same disaster, that which could happen here. Library is equally secure as a main site. Now, there is something, we have called unlabeled, the basic idea of this, is to prevent people from knowing that, you have kept a backup there.

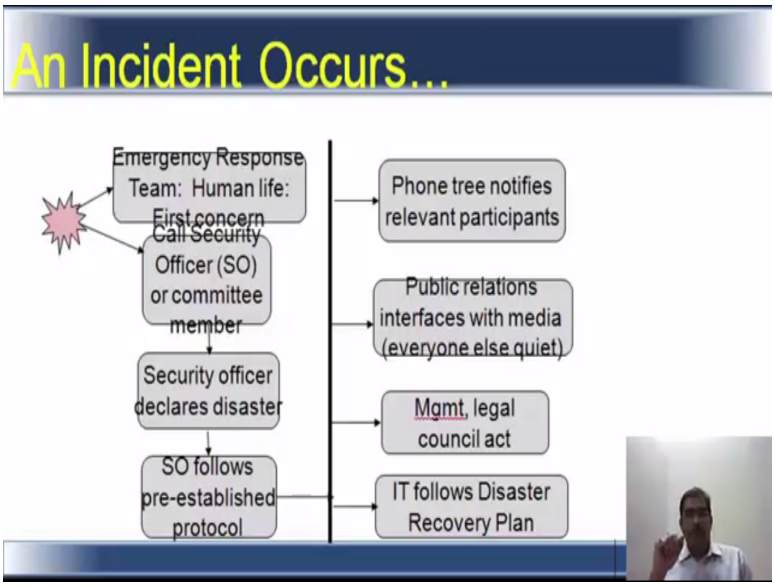
So, there used to be, checklist from the regulatory body, which specifically ask, is the data center location identifiable, or is the backup location or backup library facility identifiable, that is for the reason that, if the location is easily identifiable, there could be multiple level of threats coming in to that facility, to steal data, to corrupt the data, to exploit your network.

So, your library also should be equally secure, as your main site. Then your backup library, or your disaster recovery site, or your off site should have a constant environmental control. That is the temperature and humidity control should be there, the UPS, the smoke detector, water detectors, and fire extinguishers. As much as you have or as much as you have installed in your main site, same facility, the backup facility also should have similar infrastructure. And then a proper inventory of the storage media, and the files should be maintained which is very important.

(Refer Time Slide: 18:09)

Otherwise, you will not know what is available in the backup site. We have spoken about bcp, we have spoken about drp and we have spoken about raid backup facilities.

(Refer Time Slide: 18:23)

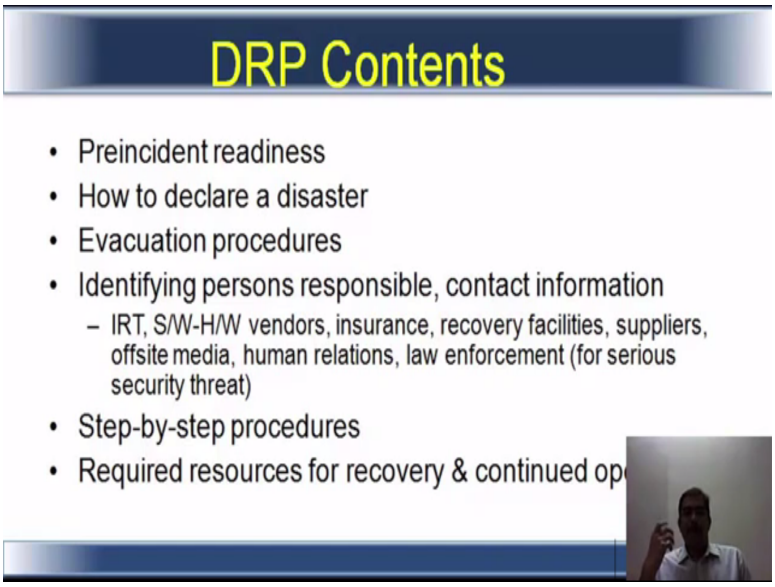


Now, how you will test all these disaster recovery testing how do we do it, take an example that, an incident occurs. Now, the activity diagram here shows that some events can happen in parallel, including all the tasks on the right. In some cases, there is a security committee, and anyone on the committee can decide, that a disaster has occurred. If you see this, it says the

emergency response team first concern is, the human life, call the security officer or the committee, security officer declares a disaster.

The security officer follows pre-established protocol, whom to contact, whether it is the police the fire, the ambulance. Then the IT follows the disaster recovery plan, the management and legal counsel act, if there is a legal violation happening, or if there is a legal viability. The public relation interacts with the media, or interfaces to the media, so everybody does not go and talked about the incident. Then the phone tree, notifies relevant participants. So, there will be a escalation procedure, where it will be specified, whom to contact, when how, so phone tree notifies relevant participants.

(Refer Time Slide: 19:50)



What are the contents of the DRP, now the basic thing is, pre incident readiness should be there, that means you will have to do mock test, and be ready or be prepared for a situation, which can have an undesirable event. What process should be followed or how to declare a disaster, what are the evacuation procedures. Most of the officers are fire extinguishers, they have FM 200 based fire extinguishers, and they have the fire extinguishers on different portions of control room.

But then, how many know to use it, in the event of an actual emergency, whether they can use it, whether they can even lift a 5 kg cylinder. Now, these are all the things, they have to be trained on. So, evacuation procedures will also specify, who will be in charge of evacuation,

who will be in charge of protecting human life, who will be in charge of shutting down systems, if it is possible. All those things are specified, in the evacuation procedures.

Then identifying the people responsible, and their contact information, it should be readily available like your incidence response team, or IRT, the software and hardware vendors, the insurance company, contacting the recovery facility, your suppliers, outside media human relation people or HR people. The law enforcement, if the nature is serious or if it is serious security threat everything should, the document should have step by step procedures, and required resources for recovery, and continued operations. With this, we will end this session, we will meet you again in the next session.