Course Name: Cyber Security and Privacy
Professor Name: Prof Saji K Mathew
Department Name: Department of Management Studies
Institute Name: Indian Institute Of Technology Madras, Chennai
Week: 04
Lecture: 11

So, generally planning requires a certain abstract statements and those abstract statements are done by those who are part of the strategic team or senior management team of an organization. So, the senior management or the board and the senior management develops value statements, vision statements and mission statements for an organization. These are some sort of the samples I have drawn here. Values means what you will stick to, in conducting a business, vision means where you want to reach in a given period of time and mission means what activities will you do, will you choose to do that aligns with your mission, sorry your vision. So, that is what a mission statement is. These are examples of companies you actually probably adore or like.

Now strategic planning is always top down , of course, there will be inputs from the bottom but planning actually implies that well, it is an activity that is led by the top . So, organizational strategy planning, I do not have to repeat these lessons because you have familiarity with this. Now I am translating this into the cyber security world, into the world of cyber security well this may already exist. The purpose of a proper cyber security management planning is to ensure that alongside this, the organization is able to plan the security organization is able to plan for cyber security management in line with the priorities, strategic priorities of the organization.

And you can see that you also need to have a structure for cyber security as a sub organization you can see cyber security as a sub unit or a sub organization of a large organization and it should have its own structure. For example, you can see that there is a role here. What is that role? CISO , that stands for security, top security officer . So, in cyber security apart from the IT, there should be a separate CISO or a C level executive, who reports to the CIO . CIO may be the head of the whole information or IT but there is an immediate role of CISO, who report to a CIO and the role of CIO is to understand both business and technology and cyber security and build policies.

Tomorrow next class is going to be on cyber security policy . The policy is something that is initiated by a CISO keeping in mind the strategic priorities of the organization and therefore, in order to draft a policy and in order to operationalize a policy and in order to build a structure and then sustain that structure, you need a top role for cyber security . And I hope in today's case, you will see that the organization you discuss did not have a

role called CISO. So then, once an major incident happens then they then they see that well, we do not have this kind of structures we need to have them, we do not have a policy, we do not have contingency planning. So, there has to be someone who leads these initiatives at a strategic level at a top level, particularly when your organization is large and your cyber assets are large and you are critically dependent on IT systems to run your business.

And you also know in India, RBI mandates that every banking institution should have a top role like a CISO role in addition to a CIO There should be a security top executive whatever you call it director of security or CISO or whatever there has to be a separate top role for cyber security alone. So, the job description of the CISO, chief information security officer does not involve that cyber security term, it is CI standing for information CISO's job description is to create strategic information security plan or the policy and plans in accordance with the policy and also prepare budgets, prepare plans, tactical and operational and monitor, comply with law, there are a lot of nuances when you actually implement cyber security in a informed way in an organization. And you will also see that when an incident happens the role of CISO becomes extremely critical as to what to do and what to communicate to the public etc. Now that is one part of planning, I stop there on the organizational planning which is alongside the strategic planning and building structures, processes etc and we will continue that path in the risk management when we discuss risk management a couple of sessions from here. But now, we switch to the other part of planning which is contingency planning.

Contingency is, you know it is an unpredicted unaccounted for incident which can happen. Unaccounted in the sense, despite all your preparation, things go wrong and those contingencies you need to have, you know in accounting we say, contingencies it is a accounting head you know, which are not planned but still can happen, contingent situation. So, as shown in this slide, the main goal of contingency planning is restoration to normal modes of operation with minimum cost, that is a goal of contingency plan. So, that is what the team, the CPMT as they are the team is shortly called Contingency Plan Management Committee. In large organizations there will be a separate CPMT team, a team which actually plans contingencies and prepares the policies and documents which we will see in a short while for contingencies .

So, CPMT team is an oversight team which typically oversees contingency planning process there will be subcommittees within, instituted by CPMT for various activities but CPMT is like a higher level team for contingency planning alone . Now what does contingency planning involve ? We have seen this incident response, disaster recovery, business continuity, this is in terms of impact . How severe an impact is in terms of money ? So, as far as possible everything should be quantified and converted to values

which are measurable in currency units , then it becomes easy in other than, qualitative descriptions. So, contingency planning essentially helps you classify incidents into one of the three and contingency planning is monitored by CPMT we also already have seen that. But what is missing in this diagram which is again drawn from your textbook is an activity known as business impact analysis.

It is assumed that BIA is contained within contingency planning, that is why that block is not separately shown but it is important to understand this . The Business Impact Analysis or BIA is the most important assessment a contingency planning committee or a CPMT initiates . That requires the committee to look at the severity of various attacks and if that happens, what would be the business impact on various business processes . Now when we analyze risk management, the other planning, basically protective, you will see that the unit of analysis will be, unit of analysis will be assets. You start with assets and if an asset is attacked, what will be the impact that is how you do the evaluation process.

Whereas in contingency planning your unit is business process you analyze at the level of business process. For example if the order fulfillment system does not work or it is hacked, what is the loss? So that is a process which is attacked or a process which is stalled So that is a process which is attacked or a process which is stalled and there is an impact for that. So you, the unit that you choose to analyze in the case of contingency planning is the business processes and the impact of incidents on business processes is what you analyze. And I will give some examples and this is available in your textbook also. Now we will come to more specifics here, the business processes and recovery criticality.

So I said contingency planning specifically looks at business processes and then they try to estimate impact in terms of time. Time is money right, the time for which if a business process goes down or there is a downtime, what is the financial impact, that is what they look at. Now in order to do that, they arrive at certain timelines and there are four standard time related parameters in BIA process business impact analysis. They are maximum tolerable downtime or MTD, recovery time objective or RTO third, work recovery time or WRT and fourth is recovery point objective or RPO. I will try to put this into a diagram so that you will better understand this but here I have given you definitions of that .

So, maximum tolerable downtime, it is a tolerance of a manager, of a process manager. Suppose there is an order fulfillment system which is an application and suppose that application stops to function , well, you ask the manager who is the process owner, somebody is responsible for that particular process , not a technical guy who operates that

business. And that person has to tell us or tell the BIA team how much time is tolerable, how much downtime is tolerable without having substantial impact on business . Well somebody would say well, one hour downtime is fine, we can manage. Of course, the process guy is the person who understands business, there is some reason why, there is some rational.

But ideally you would expect if you ask that question, if you are a BIA committee member and you go to a process owner and ask, how much you would allow your process to be down, If you ask me the question, the answer is, no downtime, we are working with critical system I know what our customers will switch to competitors, we cannot allow any downtime zero downtime that should be the MTD. And what alternate question would the BIA guy would ask, we can expect to ask. Zero can be the ideal and that is what you should say, but there is a problem with zero. How do you make the process guy think? Yeah so we will come to that, you are thinking , so you have to think and articulate. So the process guy has not given enough thought to cost.

There is a cost of downtime, there is another cost also which we will see in the subsequent slide. So MTD could be ideally zero but cannot be zero. So there has to be a recent time which the process accepts as downtime that is MTD, that is like a reference. Once MTD is established the BIA can now work on two timelines which is the recovery time objective and work recovery time. Recovery time objective is if the manager says, process owner says one hour downtime is fine, then the technique the BIA team has to say in one hour time, I have two things to do one is to restore the server or whichever system is not running to operation, it should start running it becomes functional.

The other is the operations restore, system is ready does not mean that the operation is ready, you know you have to do a lot more preparation to start working on that . So there is a work recovery time and there is a recovery time objective, RTO is, well, server is now ready for use, then the operational employees come and then sign in and then do their formalities, do the checks that is required that is another time which is called work recovery time. And then you find that you know your operations cannot be, cannot be starting from the instance it went down because we do not have a backup . So it it may take more time actually to come back to normal operations depending on some of these aspects. So therefore the fourth timeline is coming which is recovery point objective.

RPO is nothing, but the point in time to which a system can go back, this is purely dependent on the backup policy. If you are backing up the system every hour so maximum one hour data may be lost so your RPO is one hour, you can go back to one hour maximum . But if your recovery policy or your backup policy is for everyday one backup then you may not have that much privilege. So, RPO depends on the criticality and these are

timelines set by the management to manage contingencies. So, BIA team's responsibility is to ensure that these timelines are set if they do no exist.

And then based on say an MTD which is the overall acceptable downtime, determine a rational RTO and WRT and also establish an RPO, a backup policy. Once these things are done, then you can go forward. So, this diagram actually illustrates the four time related parameters we discussed MTD is the sum of RTO and WRT. RTO is the time taken to bring the system live, the system goes live here and it becomes operational here. So, RTO and WRT together is MTD and MTD is a time accepted by the process owner, not the technical team.

And RTO and WRT are times that are worked out by the technical team based on how much time is allowed to go down . And RPO is again the recovery point objective is a backup policy and also depends on criticality of the business . Now this is again an illustration of the concepts we discussed. We already saw that BIA, business impact analysis uses business process as a unit . So, one should first identify which are the business processes in the organization which are automated by applications.

Business processes are what get automated by applications. So, a invoice process is automated, you know it is using applications. Suppose the invoicing goes down, it has an impact on business, then you pressurize the process guy to specify what is the MTD . How to pressurize, we will see in the next slide . He cannot, he or she cannot give 0 hours and some rationale is worked out , 72 hours is what you can tolerate maximum.

There will be losses but this can be tolerated maximum. And then you can see that they work out subsequently the recovery time objective is 36 hours which is less than, the RTO will be less than the MTD obviously because WRT is also involved. You can see it is 36 which is half the time . So, half the time is allotted for work recovery. So, so but this need to be worked out for each business process.

So, you can see the role of a BIA team in contingency planning is to analyze business processes which are automated and arrive at this timelines and then work on further processes which we will see. And here in this particular illustration you can also see that they use FIPS 199 which you are also going to use in your incident analysis in your assignment. So one could also determine the severity in terms of confidentiality, integrity and availability as low, medium or high . So, that gets documented in a process like this. Based on this concepts let us go to the next item which is about the cost balancing.

So, by now we are clear that contingency planning involves business processes and contingency planning involves time which is downtime. And downtime means cost, but

here in this chart we are saying downtime is not the only cost, recovery also is a cost. If you have to restore business processes which is disrupted back to operations, again the cost of recovery is a function of time. If you say 1 hour is what you can tolerate, BIA team can say yes 1 hour, but the cost of recovery can be very high, you may have to have a hot site always ready or a warm site ready . There has to be a parallel system for which investment has to be made.

We call it redundancy, to make the system available you need to have redundancy. Redundancy is a cost. So, you can see there is a optimum time that has to be worked out to balance the cost of recovery and the cost of disruption . So, length of disruption time is the x axis and cost is the y axis. So, when length of disruption time is made low say a region like this , disruption time is made as low as possible by ensuring redundancies and you can switch over to a new system immediately etc, very good.

But your cost of recovery in terms of systems that you have to keep ready for fast recovery goes up. So, the cost is borne by the organization right. The process owner can always say it should be here or here . Then somebody has to show this graph, well Boss fine, I am fine, but we have to see if the organization is willing to invest so much to reduce the cost of recovery. So, therefore you can see the trade-off between cost of recovery and cost of disruption which will be the typical scenario and therefore you know the optimum point is the point of intersection between the two graphs.

So, this concept should be clear in the mind of managers because ultimately it is a negotiation for time. Contingency planning is basically a negotiation for time. In how much time you objective is to bring back the system back to normalcy, minimum time at the earliest. That earliest is the objective given by the management, that earliest depends on these two aspects, cost of recovery and cost of disruption and how much you are willing to invest. So, contingency planning cannot be done without the involvement of management and their willingness to invest in redundancies, to ensure restoration of systems based on priority .

Now this so, rest of the contingency planning in terms of what you do can be understood using this diagram or this particular block diagram very well. You can see that there is a switching from IRP to DRP and DRP to BCP depending on the impact of the incident . What is the impact of the incident on business processes determines, what action is triggered? An IRP is triggered if the impact is low. It switches to disaster recovery, if it is next level and it switches to BCP business continuity planning, if you cannot continue business in the same location. So, I would say this will be led by, it also depends on who leads the initiative or who leads this particular activity or task.

This will be typically the CEO, because you are shifting, you are moving from one place to the other . This can be by the CIO, there is a major incident, but your contingency planning says that this can restore to normalcy within a few hours. So, you have an estimate of that, it is not that you have to switch to another place . And this can be done by tech, this is a small incident. So, the impact determines whether it is an incident or a disaster or a BCP.

So, there actually there is a difficulty in the articulation because the terminologies whoever gave it, is not well done . Distortion and disaster, well, these are two you know, it characterizes the incident, but BCP is the process. So, you can only say business continuity is a total disaster sort of thing, highest disaster. Yeah, you can also say the restoration is in the same site, in the disaster recovery. It is in the primary site, you do not change or switch the site.

Now rest of the activities involved in the planning are descriptive and they are described in your textbook. I will take you through these slides which describes them, but they are easy to understand, self-explanatory most of them as to what you do before, what you do during and what you do post etc. So, for familiarity, I would take you through these slides and what is incidence response plan and what is incidence response, as to what you do and how you do is the plan. And we have already seen that it is a reactive measure, fine. And IRP has three phases as I said - before the incident during the incident and after the incident.

For example, during the incident what is the protocol, post incident, you need to document the incident as to what happened and there has to be a structured documentation of any incident that happens. So, these in a organization which follows the CP should follow these protocols or these rules in cyber security management. So, all this should be available, the plan should be available prior, if the IRP has to be implemented. And during the incident of course, you have a procedure, for example , if it is identified as something that requires shifting the site, the BCP comes into picture and the BCP follows a process. And that is the BCP documentation or BCP binder and who should be contacted etc are all well described in that document.

And after the incident of course, you document and then move on having restored the system. And there is also the question of how do you actually detect incidents. Intrusion detection or intrusion detection systems do exist technologically and therefore, the system should be active and you should have active logs and active reporting systems. And conceptually Pipkin and others identifies three categories of indicators for incidence. They call it possible indicators, probable indicators and definite indicators.

May be the incident that we are discussing in iPremier is throwing some light as to some things can be an indication of a higher disaster that is going to happen . So, they are probably indicating something worse, the future can be worse than what it is now. So, there are indicators of these categories which requires expertise and experience to use . And some of them are actually described here . Change to logs for example, is a definite indicator of something is going wrong.

Yeah, threat intelligence so, well incident means something that has happened. Threat is something that is, that could happen. So, both are different. So, here we are talking about well, something has happened and even after happenings if you do not have systems, you may not know .

But what indicates incidents is what is described here. So, we are talking about threat intelligence which is about what potentially can happen . Incident response, well described here as to how you respond and you should have people, process, technology essentially to respond to situations like the alert rooster, alert message and so on, how you communicate it to people once an incident happens etc. And an incident should be documented in a structured format and that should cover what, when, where, why and how. So, there should be structured templates or documents which are available when you actually implement standards for cyber security. Well, here is a example of a incidence response plan by Carnegie Mellon.

And the idea here is to help you appreciate how detailed it is. An IRP document can be very detailed getting into definitions of course, intro definitions, roles and responsibilities, methodologies, different phases in incident response and guidelines for the incident response processes. So, these activities are documented in a very detailed way in leading organizations. Also there should be clear documentation as to when an incident becomes a disaster and when a disaster becomes a , BCP category. And there should be, if these are all management processes , there should be after action review as to does it improve or does it become worse.

So, and this point is very important . We come to this important point which is law enforcement involvement. In the case that we discussed in the last class, there was again lack of clarity as to should it be informed to the government or can we contain this within the organization. And that clarity should be there with the organization or how to decide. And when we discuss regulations particularly of the kind GDPR which is prevalent in the EU countries, by regulation it is required that an incident be reported, it should be reported to the government.

You cannot hide it under the carpet, it is against law. So you do not have a choice, but

you can make a case by suggesting that this was not known or why it was not disclosed, there has to be a clear case. Otherwise the law requires that, GDPR requires in 72 hours, a cyber incident should be reported or 3 days, in 3 days the report should be given. So therefore, there has to be sufficient knowledge for a cyber security management organization to determine reporting to government and reporting to public . And law would require that , so that aspect is also important. And disaster recovery as the name indicates is based on the severity and this is major incident.

So you can think of the iPremier case which is a major disaster, business is down, right. And they do not have a BCP of course, they have to manage within the site and that discussion is on. Let me actually leave these slides for you to read and these are taken from your textbook, I do not want to spend time. Unless there is something that I need to describe you in a lot more detail, BCP and DRP we have already defined what they are. And in BCP there can be many strategies, you can have a hot site, you can have a warm site, you can have a cold site.

Hot site means there are say, 2 sites running parallely, if one is down the other is ready to run. So you are very, you are ready to restore your business processes, may be certain business processes which are most critical immediately, there is now a very, very low down time. That is known as the hot site strategy, warm site is well, not immediately ready but can be made ready within defined timelines. Cold site is the lowest but there is a site possibly you can actually bring into operation within a longer period of time. And then there are other options in cyber security management parlance today to use sites which are time shared, lot of options which requires expertise and knowledge of the domain to determine.

So what it means is BCP is a separate strategy for which you need to know the market, you know you need to know what are the possible options and then that knowledge should be available within the organization , within the region where you function. Alright, these are self-explanatory, I move on . For the benefit of time I would leave this for you to read. Yeah, let me come to this point and close the lecture here and then we will discuss the case. Testing contingency plans, so are we ready if an incident happens ? So this is again the role of the security organization to keep the organization alert and ensure that they are ready if an incident happens.

So there should be periodic checks , sometimes mocks, to test the preparedness of the organization. And I have given you a link here which you can go and explore to understand practically how some of these tests are done in organization. You must have heard about red teams, blue teams and purple teams . Red teams in an organization plans a simulated attack, blue teams defend, purple teams moderate . So how the attack could

have been better or how the defence could have been better, so they learn lessons from it and then go further on.

So this is a sort of testing process through emulating potential incidents. And I had a practicing cyber security manager who came and did a drill like this for the students. We will see if that is possible this time. So these are the practical ways of continuing to ensure that contingency planning is done and it is active and healthy to face up an attack or an incident if it happens. Do you have any questions? Or for at this time I would suggest we switch to the case.

So I would have the next team to come and present and discuss the case, iPremiere B and C. Thank you.