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: 10

Hello and welcome to Cybersecurity and Privacy course and today's topic is Contingency Planning. So we are building foundations for cybersecurity management, so we are trying to understand fundamental concepts and we are also looking at cases as part of this course to also understand what is going on in the environment and to connect of course, principles and practice together, that is the effort in this course. So we will discuss the different aspects of planning as a whole in cybersecurity management and understand a wholesome aspect of planning first and then specifically go into contingency planning in today's session. There is another aspect of planning, which is for risk management which will be in another session. So both have different objectives and I think I highlighted this already, one is preventive, other is reactive. So today we look at reactive, okay, incident happens then what you do, okay, that is what contingency planning is, the other is incident should not happen, so you try to protect, so that is a separate path.

So we already discussed in detail the case of iPremier company in the last session and we understood how a company which is very ambitious in terms of future prospects, very professionally managed company actually got into a great shock, you know it is not just an incident of low degree but something of a huge shock in the early morning hours, okay. So incident happened at 4.30am, if I recall correctly. So I think we also discussed, a drone attack in Saudi Arabia on a refinery which also happened almost at the same time, 4.

15 or 4.30. So in India we call it Saraswati Yamam, right the morning, the time when we actually sleep or it can also be a time when you can have very high productivity mentally. But essentially that is the time when the world is sleeping mostly and that is the time, the hackers choose to shock organizations. So and we also saw how the company was ill prepared or not prepared at all to face something of this kind and then you saw, since there is no plan to follow in the event of an incident, nobody knew what to do, Everyone was actually asking the other or suggesting the other and worse, try to protect one's own jobs or one's own roles.

So that is what happens when there is no plan and we do not have clarity on things, okay. So contingency planning is essentially to address that aspect of what to do if things go wrong. We wish and plan such that, things do not go wrong, but despite that things can

go wrong then what course you take, that is the essence of contingency planning and the case teaches us that this contingency planning is very important. There can be several scenarios like Target Corporation despite having invested a lot, invested a lot in cyber security, still breach happened and here is iPremier company, which did not care about it and it happened. So it can happen and it can happen and therefore the point is, there should be a clear plan that actually, in case of fire, for example, you know what to do.

So there are oftentimes you know the fire or the safety department actually gives context drills, you must have seen that you know, they create fake incidents and try to sort of alert people so that they ensure that the protocols are followed in the case of an incident and they are able to restore the organization to normalcy, okay. So that is the purpose of contingency planning. So let us move on. Yeah, so it actually, Gilbert very well explains what happens if there is no contingency planning, right, like the iPremier company. Yeah, so you just have to yell or in theory, they call it emotion focused to coping.

You do not know how to cope, you cannot use your, mind does not work because there is no clarity, then you actually become emotional. And then you call for help or yell or runaway or wish that there is nothing wrong etc. So these are our, tricks that our emotions play and we have to be very careful. As managers your responsibility is to protect the assets of your organization, number one. Number two, also if an incident happens to bring back the operations to normalcy at the earliest.

So these are very important as far as cyber security management is concerned. I just add a small insight from another case again, published by Harvard Business School. The case actually discusses about a company called IVK, something like iPremier and IVK is an established company and there is an IT department there. And there is a newly joined IT director, who after assessing the preparedness of the organization for cyber security challenges, suggests that we should, the company should invest more in cyber security. And apparently, the director of IT made a proposal to invest in a Intrusion Detection System or called IDS.

In yesterday's case we saw that there was an incident happened but they do not know there was an intrusion or not because there is no intrusion detection system for reporting it. In the case of Target Corporation you know, that there was an IDS but it was not, actually it was turned off. So but there is no IDS at all. So IVK's director wants the company to invest in something. So you know, in corporations you can, as managers you can propose capital budget projects, new projects, revenue budget and capital projects, capital budget.

In capital budget you make proposals for new systems and when you do that it goes to

the corporate office for evaluation. So then there will be a steering committee or a high level committee who actually looks at project proposals that has come from different departments or different functions and then prioritize them. So evaluation and prioritization of projects is a corporate task. And what happened to IVK's IT department's proposal was, the proposal was dropped two years, consequently two years. And the steering committee said, " No, we do not want this project, we do not want to invest in this project.

" So the reason, reason is given by the finance department or the you can imagine the CFO. What is the return on investment? If you invest in an IDS or a latest firewall, how does that money come back? Suppose you invest 100 rupees, for a finance guy, the 100 rupees should come back, say in 3 years or 5 years, as 150 or 200. So you have you should get more money than what you invested then only it makes investment sense okay, business sense. But in the case of security systems does it give any return and then why should a company invest in it? So you can quickly share your thoughts. Sir, it does give a return but then there is no definitive period or time frame when the returns will come, the return will come in the form of intrusion getting detected, your data being safe, so that you are able to take evasive measures at that point of time to safeguard your data or critical information which can be in the form of credit card information, financial, banking information such thing which will cause larger impact in the long run if that information got out into the domain.

Well you may be right that is the same argument the IT director must have given, if we do not invest in it, we may have this loss, that loss, goodwill loss and so on. But the finance guy will ask well, tell me how much money you get back ? Show me the ROI. So the message is, you quantify it. So they can say IDS costs this much, say, 5 lakh rupees or say 25 lakh, whatever. So, 25 lakh given, what is the return ? Give us money.

They want 25 lakh as 30 lakh, How it will flow back ? it should be quantified over a period of time. How will you do that? Sir, in this case, in case we want to quantify, what is the return which we will get ? Is it, will be in the terms of, say, suppose the information gets leaked, then what kind of that legal ramifications would be there, how much that would cost the company as in the case of iPremier, the legal advisor was advising that we are likely to go into lawsuit. So that cost is there, then secondly in the event of some critical information getting leaked, some patent information or something, what is the cost of that, the company which has already spent on it, that will be the cost factor which somebody else will not need to spend. So if we want to categorize it, so this is how which somebody else will not need to return. Okay, okay, okay, okay, I think you are thinking in the right direction.

Is there any other answer, just to add on to that yeah, take the mic, We could present it as 2 scenarios, if we do not make this investment, what the, what this kind of an event can lead to negative sales impact over a period of time versus if we make this investment, the sales impact and the legal cost taken together would be much lower. So this will have a lower negative ROI compared to doing nothing. This is what you are suggesting right, there is a cost to the company if no investment is done. How do you estimate it ? This has to be estimated, this has to become numbers at the end. So that is consultant's job, right, you have to, in order to convince the management, you actually have to collect data, you have to sample, there has to be some sort of sample data that you use to arrive at this figures, potential cost involved if cyber security systems are not in place .

yeah you are saying something, yeah. Like they can estimate the number of incidents and how long will it take to fix and what will be the cost to fix those incidents. Okay. Okay. So similar company, how much, what is the probability of it being attacked and how long will it take to recover.

Yeah. How long will it take loss of revenue because during the period, you know website is down, all these can be added up to give a number. Yeah. Yeah. Yeah. So I will say there is a difference between these two, right and what do you think which will be higher, which cost will be higher ? Yeah.

So I will say there is a difference between these two, right Yeah. Yeah. Yeah. So I will say there is a difference between these two, right and what do you think So you are actually trying to minimize cost here, okay because there is no revenue, no revenue that you are generating by investing in an IDS or in security system but you are trying to reduce cost. So which cost should be higher ? Ideally if there is no investment, the cost will be higher okay, so this will be plus plus, this will be plus okay.

So what you are trying to rationalize is, how much cost will be less if you invest in a system or in a upgraded security system and that reduction in cost should be much higher than the investment that is required. That is the rational for any investment right, You save more than what you invest, then the finance guy will be convinced but where you know where the director went wrong is that, you know, he got disappointed because the company is not willing, despite me giving all the reasons. So still qualitative compulsions or arguments do not really sell for finance department they actually require quantitative, proper quantitative rational yeah. Again Sir, the question is how much to invest because it is not one time investment.

Yeah. It has to be you know every time upgraded, so it is something like dynamic cost. Yeah, yeah, so yeah, this is dynamic absolutely. You can see as the environment becomes

more fluid in terms of cyber security it becomes increasingly difficult to make this assessments. So we are going to discuss this topic in more detail in risk management because that is essentially at the end of risk assessment, a company has to determine how much to invest and that should be proportional to the risk okay and that exact assessment of risk is the highest challenge. And you can see the difficulty in this estimation, in the absence of cyber insurance in our country.

It is very difficult to get cyber insurance done for cyber security risk and that is a field still emerging and if you read literature on cyber insurance which one of my students is working on a project on cyber insurance. So we find that this is an area which is of very high importance but very difficult, due to difficulty in exact assessment. So you are right, this should be the way theoretically to do this but making this estimates accurately would be a challenge. So these are, this is related to the environment but doing nothing is not an option, you need to have reasonable safeguards and the senior management should be educated to understand what is this cyber security and why it is important to invest in it, basically to save costs not for new revenues. So that is an understanding finance guys need to have , you know it is not like it will attract more customers or things like that or you know, more sales, nothing of that sort is not going to happen there is no new revenues stream that is generated but it protects.

So you can see that the two cases both iPremier as well as IVK points out that the cyber security was a low priority for the company and that low priority by the senior management actually resulted in the situation that we saw and in the IVK's case it was the inability of the IT department to articulate the savings from cyber security investment and from the senior management's perspective, it is their lack of understanding about what cyber security challenges are and that also requires more understanding. So again, I think this is again Gilbert so this is well illustrated if you do not invest in cyber security what people resort to because technical people knows what can go wrong and they will be very disappointed, you can see we have more cases coming up in today's cases you know, how they are actually worried because they know, and they try to do something, to protect the organization. Managers or non IT managers may not be able to appreciate that. That brings us to the topic, so we are going to discuss contingency planning. So before that, what is planning? Planning is the integral part of management, what is a manager's role? Basically to manage resources and how does a manager manage resources? Planning, proper planning, so proper planning is fundamental aspect of any management.

So if the planning particularly in the context of cyber security is to align with the goals of the organization. So essentially organization wants to go somewhere, the iPremier wants to go somewhere in terms of its market competitors and future, but if he has to go somewhere, it also needs to have cyber security to protect its cyber assets so that it is

able to attain its goals. So the purpose of cyber security planning is to enable an organization to achieve its goals, its business goals. So the cyber security planning is very much related to the goals of the organization in that sense and you also know from theory already that if you plan, it helps you reduce losses or optimize your resources and it also enables you to coordinate and that coordination will require proper structures within the organization. So all that is a part of planning, and you know this great person or one of the founding fathers of the United States, who said " If you fail to plan, you are planning to fail.

" Who is this? Yeah, Franklin Turbolton, you know there is an investment banking company so they are all sharp finance minds who also said time is money, right. So it was Benjamin Franklin and it brings us in abstract terms how important planning is and again in abstract level also, let me actually put this as to how when you make high level plans for an organization or a mission, you also keeps gives importance to safety or security. You must have heard about moon mission, right who actually charted the moon mission somebody gave a talk in 1961 in a university, before this decade ends that is the 1960s, America should send a person to moon and getting back safely. It is not about you send him out there, does not matter what happens, okay bring him back to earth safely, okay. So you can see how well documented or well thought out is this mission .

Safety is given paramount importance in that statement. It is not about showing a, you know, running a victory flag in moon and ending there. So this is essentially what planning at a higher level means, the consideration for security should be embedded within the goals of the organization, okay and this was Kennedy, John F Kennedy, and when did this really realize? This was 61 and when did man land in moon? 69 okay, July 69. So did this happen, it did happen well, that is separate project it is a good case for project management. So information security planning - there are two types of planning as I said already, contingency planning and organizational planning.

Let us look at the right side first, organizational planning consists of three categories Operational planning, Tactical planning and Strategy planning. This you must have already studied in management lessons, basic management lessons the order is not put correctly in the textbook. So I have just copied it as it is, but it should be operational, strategic planning, tactical planning and operational planning in terms of range, time range. So the organizational planning for business objectives is one aspect. So there has to be cybersecurity plans alongside these different types of plans.

So for example there should be a strategic plan for cybersecurity, there should be tactical plans and there should be also operational plan which is day to day activities. Day to day monitoring versus say medium term plans which are tactical plans and long term plans,

typically 3 to 5 years which are strategic plans. So cybersecurity planning should align with those plans, that is one aspect of planning and it is in that planning you take care of the risk that is faced by different assets of the organization and make your planning to protect and prevent. Essentially this kind of organizational planning is to protect and prevent potential incidents. Your it is basically to safeguard yourselves but when you come to the left side, the objective is different.

The objective of contingency planning is essentially to restore systems, restore the operations of an organization to normalcy in the minimum time, meaning that it assumes that an incident has happened, and if it happens, what do you do such that the operations are restored with minimum impact. That is objective of contingency plan. So contingency planning are, is of 3 types - incidents response planning, disaster recovery planning and business continuity planning. In short they are called IRP, DRP and BCP. In the iPremier case you must have read somebody was saying we have a BCP binder but we do not know where it is.

So BCP is a type of planning in contingency planning and let me summarize you, summarize this for you here. What is the basis for deciding whether one should follow an IRP, DRP or BCP? The basis is the impact, okay. How much impact a particular incident has ? So there can be low impact incidents in the systems of a organization. For example, somebody detect detected a potential virus in a one localized PC. So one PC is not working or something is not running.

It is an incident we should, the the technical team must be alerted but operations are going on. So it is called an incident and how you respond to that incidence is the IRP. Low impact incidents. The next level is the disaster recovery. Disaster recovery incidents, they are also incidents but they are of higher impact.

For example, some operations are shut . E-commerce operations is not running, and therefore it is impacting the organization's business or transactions. But it may not require the organization to shift its operations to another site. There are incidents of that severity where you cannot continue in the same site at all which is known as business continuity planning. In you know you are all familiar with the Chennai floods . Every IT company was moving out of Chennai, and there was a big planning that was required at the organizational level, at the leadership level.

So the extent of impact in a BCP is the highest, and that is a call an organization takes. We cannot function here anymore. It could be technology reasons. It could be otherwise . BCP is a generic term where organization has to shift its location.

Disaster is high severity but you do not have to move out from here. You can restore to normal operations after some time. So incident is minor. There is an incidence but operations are going on. So this obviously shows that there has to be a management effort to determine the impact of incidents and to classify them based on that impact assessment and then move to appropriate action.

For example if you take iPremier's case, there should be some basis to decide whether it is a incident or a disaster or a BCP or a business continuity situation. What is the case and then follow that guidelines immediately . So yeah, so this is my own diagram. This is not from the textbook to illustrate the various aspects of cyber security incidents.

We are talking about incident. What is an incident? An incident is a attack, a particular thing that really happened and why incidents happen? Incidents happen through certain vulnerabilities . If you look here, an organization has assets. In cyber security, they have cyber assets.

It could be your data center. It could be even your people. But that is what is targeted, by the external world. There are hackers or the negative world and they are looking for opportunities to enter and distract or destroy your systems. And they enter through these gaps . There are many gaps. There are potentially many gaps in the firewall that you have set up or in the walls that you have built around your data center, physical or virtual .

But these are all gaps are called vulnerabilities. And a hacker may use a particular exploit . Hacker exploits a particular gap, and intrudes into your system . Once the intrusion happens, it is a incident. Sorry, this become an incident.

And an incident can be of three types. One is low, medium, high. That is what we saw as impact of incidents. So the extent of damage, that is caused. And therefore based on the impact of the incident, some action needs to be taken. Once this kind of an incident happens.

So that is the purpose of contingency planning. And so what is illustrated in the picture is, somebody is walking And you can see the sole of the shoe, right. There are knurls on the shoe. So it gives grip on the road. So that is sort of protection. Somebody has taken precautions, even if there is a banana peel on the road, you may not fall.

But it depends on the extent of slipperiness Because there was a rain also, you know, you may fall actually despite all the protection that you have taken. So this is a picture that you can keep in mind in my own way of illustrating, what is a cyber security incident.

You have protection but despite that there are vulnerabilities and hackers can exploit that and then there is an incident. And if an incident happens you need to respond .

This is the contingency planning . Deals with the incidents. It deals with the incidents.