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: 08
Lecture: 22

Hello and good morning, welcome back to Cybersecurity and Privacy course, we have been discussing a risk management, cybersecurity as a risk to be addressed for appropriate solutions, that is what we discussed in my previous session, I know you had a session with Mr. Sai last week and I am hopeful that you could get lot of insights from experience, from practical experience in handling cybersecurity issues. So that is one aspect that complements the theoretical, conceptual inputs on cybersecurity management. So today, I plan to summarize what we discussed in risk management and then close that topic and then move on to cybersecurity technologies. So the topic for today is to give an overview of technologies that are used, particularly for protection. So we have seen different roles of technology but we would intently look at the protection role of cybersecurity technologies and then of course, we will discuss a case on defense, especially we are looking at technology today from the defense point of view, How can you deploy technology for defense against attack? So risk management, so in risk management we saw that risk management is basically a preventive measure, we try to identify assets because assets are that which are attacked or become the target of enemies.

So therefore we found that for risk management, there are three stages, the three stages are one, you identify. You identify yourself and you identify your enemies. So essentially you identify your assets and you also identify the threats, potential threats and then the next stage is a assessment. So assessment mean, it is all at a quantitative level, you try to measure you try to bring some sort of precision to each of these categories.

So you have identified your assets but how do you value them ? So if they are affected, what is the impact, what is the financial impact and therefore there has to be some valuation of these assets. So that is one aspect and then you also look at threat intelligence, what is the probability that particular threat would materialize and you know, threat would occur and if that occurs what is the chance that it will be successful, given your existing defense systems? So we actually finally discussed two important measures that are used in assessing risk. The loss frequency and loss magnitude, loss frequency and loss magnitude and we found loss frequency as a product of probability of an attack into probability of successful attack, success in the sense, it actually

happening in your system. So that is loss frequency and loss magnitude is the exposure of a asset. So asset value multiplied by how much, what percentage of that asset will be exposed.

So these are actually measures that one need to have and once these measures are developed, you can actually arrive at the final measures for calculating risk. So we also found that risk is an overall measure or we call it residual risk, the risk that is left after implementing certain protection mechanisms, that is the residual risk. Residual risk is the product of loss frequency and loss magnitude minus the protection from existing systems plus a measurement error, a measurement uncertainty, not just error, you can actually calculate measurement uncertainty from the error. So that is the residual risk in a very detailed level of quantitative measurement. So assume that you have assessed risk for each asset.

So we, the unit is asset, so you go by asset, so each asset has vulnerability, each asset has a value, so you know, you actually arrive at the vulnerability by mapping each asset to a threat and then you assess the vulnerability of each asset. So we have a TVA worksheet and finally you also calculate the risk pertaining to each asset. Now this is actually placed before management. So the management is given the information, well you have so and so assets and these are the risk under which they run. So the management has to take decisions on risk management.

Finally risk is something that needs to be managed, you have made an effort to quantitatively estimate risk for each asset and you say, your so and so asset, asset X is having this risk in a relative scale. Now, so what, what do you do? Action has to come from the management, you are informing the management you are running at so and so risk, some have low risk, some have very high risk, some have medium risk and so on. So what are the options in front of the management to manage the risk? So there are five options for risk management, that is what is depicted in this slide. You can see, the first option is defence, second is transfer, third is mitigation, fourth is acceptance and fifth is termination. So it is not just one option, defense is not the only option, often times we think that cyber security is to develop defense systems.

But you can see in management literature, defense is one of the options and that is not the only option. A management when it is informed about the assets and risk and a comparative scale for all the assets, it could take a call in any direction and that has to be, of course justified as to why are you taking a particular path. So a justified path has to be taken for managing risk. So defence is essentially, well you find a risk, your e-commerce server has a high risk and you just do not want to leave it as it is. So you immediately want to step in and put in place safeguards.

So you decide to invest more in cyber security technologies, you decide to recruit a CSIO, so you may invest in people, you may invest in technologies because your decision is to defend. So if an attack occurs tomorrow, we want to be fully prepared or as prepared as possible. So that is basically an effort to reduce the risk. So when you increase your defense, you are basically reducing your exposure or reducing the chance of success of a attack and therefore you are actually building a defense against potential attack, option one, that is an investment decision. Transferal, can you imagine what is transferal? This is another management option and it is a very smart option and this is what many non IT companies would do about their cyber assets and that is essentially to transfer risk from the owner of the asset to a third party.

Outsourcing, essentially outsourcing, in outsourcing the management of your IT assets is transferred to a third party vendor, a service provider. So look at say, TCS providing IT services to a US client. So it takes responsibility for the running of the systems and there are service level agreements. So what the client want is that the system should be available at say 99.99 percent and so on.

So that is the responsibility of the service provider to ensure that the system is available. So cyber attack is something that the vendor needs to manage or the risk of the owner is passed on to the service provider. So that is one way. What do you think about cloud computing? Today's storage has moved to cloud. He is talking more of transferring this entire data management and everything to cloud computing wherein that would be actually a third party vendor.

Because if we see, transferral itself becomes a superimposing topic which includes all these defense, mitigation, acceptance, termination itself and because it is a very broad based when you transfer some, the entire risk management to someone, as a transferal, like TCS or so, then they start taking care of all these aspects from defense, mitigation, acceptance and termination. They may, but each of them are separate strategies, you may still own. So a company can transfer, it can also choose to own. So then the mitigation is actually the responsibility of the client. So it depends on what choice.

Once the risk is transferred, the vendor may try each of these options again because they have to manage the risk. So that is right. But yeah, that is but the client can continue to own the assets and take one of these options, option other than transfer. Can we say that transferal basically means, more towards this cloud computing? Cloud is one option. There is something called managed services in IT.

You are from the IT industry. What is managed services? Say Wipro or TCS, manage

the IT services for a third party. What that means is that the assets may still be owned by the client, in terms of the material ownership but the services are managed. It is for the service provider to ensure that the system is available. So cybersecurity management of the asset of the client becomes a responsibility of the service provider.

So that is another model that is called managed services. So there are different options available for managing cybersecurity or transferring the risk to a third party and then we sort of you know, we do away with handling it yourself because oftentimes you do not have the expertise, internal expertise to manage cybersecurity. So you give it to a professional who can do that. You have a point. In this transferal model, actually then, still you know, we might be unstable to the customers, we might have transferred.

Yeah. As I have mentioned. Yeah. You recall a case right which we discussed, which is the case of iPremier. In the case of iPremier, the company had transferred the risk to a third party but the third party was unprofessional. They were actually not updated.

They were even worse than the client's knowledge about managing cybersecurity. So therefore it has to be professional management, of course. So let us move on, the third possibility is mitigation. Oftentimes we use the term mitigation and risk management synonymously with defense. Defence and mitigation are two different strategies.

Defense is where you build defense against attack. You build a firewall against possible attack, that is defense. But what is mitigation? Mitigation assumes that attack has already happened, as in contingency management or contingency planning. So in mitigation, having an incident happened, how do you minimize the impact? How do you actually minimize the impact of an attack? That is the effort towards mitigation. So risk mitigation means you are not building defense systems but you are trying to minimize the impact of potential attacks.

So for example, if you invest in contingency planning, you actually create a team for contingency planning, you invest on a hot site. Are you defending? It is not an investment in defense. It is an investment in reducing the impact and therefore it is a mitigation strategy. So you have to look at it from two aspects, you know in terms of managing risk by the client, of course. One is to invest in defense technologies, other is to invest in mitigation.

Mitigation means how do you reduce the impact . So those, you know, so separating resources or allotting resources for contingency planning and having contingency planning in place, is in itself, is an investment on mitigation or it is a mitigation strategy. So that is the third option. So defense and mitigation are different, keep that in mind.

Oftentimes it is used, I have heard people using it synonymously but it is not correct.

Mitigation is reducing impact and the fourth option is acceptance. So you can recall discussion of some of our cases like Target corporation. So some experts suggested, why bother so much you know, you are say 70 billion company and you lost 500 millions. That is a small tip and does not matter. So do not over invest, do not do anything about defense or mitigation, do not invest further on cyber security.

We will face or we will cross the bridge when we come to it. So but keep in mind, these are all informed management decisions. Therefore, if your choice is acceptance, you should know the economic implications. So how much is the loss and how much is the gain and there has to be a economic justification for opting that path. So you know, so you can imagine conditions under which an organization may just be ready to accept.

So I think to a large extent, academic institutions like ours, have chosen the acceptance path, in the sense, we are not too much worried about cyber security, cyber attacks and if something happens tomorrow, your data is leaked or hacked, well we will face it. So it is not such a critical thing. So we just will accept it. We will see when this happens because we do not have so much of investment in cyber security. So it is an acceptance strategy based on, sometimes based on the criticality of data, criticality of applications etc.

And the fifth one is termination. Termination means, well the investment in cyber security has to be so much that it does not make any economic sense to have that business unit or have that business. So the cash flows or the revenues versus the cost, does not justify in having that business itself, you may terminate the business. You may stop having or you may do away with those IT assets. You may actually sell it off. That is also an option, based on economic justification.

So five options before management and an informed management, a rational management should take decision based on economic justification. So what is the economics of it? So let me go ahead and conclude this. So risk management strategies aside, as I showed it you from the textbook, using the textbook language but there are different standards which use, may use a different terminologies for the same thing. For example, a standard for documenting risk given by NIST is SP 830, that is one.

So they use a slightly different language. You can see the equivalent language there. ISO uses a slightly different language. So this table summarizes them. So essentially the generic concepts are drawn from the textbook, you can see it in the first column and then standard specific nomenclature could be different. And you may also note that

there are standard ways of documenting risk, once you actually assess them.

So as I just said, controls is something that needs to be justified, essentially economic justification of cost and benefits of each option. So as students of management, you must always, already be familiar with cost benefit analysis. For any investment decision by a management, you actually look at cost and benefits and the simple argument is that the benefit should be more than the cost and how much it should be more than the cost, actually is often used to, you know, to give a go ahead to a project or no go ahead to a project. So gains should outweigh the cost and that is the basic principle in justifying cyber security risk management options as well. So when you take a particular decision, say investment in defense or investment in mitigation mechanism, it is a actually an economic, economics is involved, you are putting money into it to build certain systems, to protect or to reduce impact etc.

So you need to actually arrive at a cost benefit sheet for that each option that you have and one of the form, one way of doing that is shown in this slide, you can see you can note that you first use a, you first arrive at a term called annualized loss expectancy, Annualized loss expectancy, in the next slide I will show you, how to use this measure to calculate the cost and benefits. So annualized loss expectancy is the annualized loss magnitude, SLE is nothing SLE, single loss expectancy is nothing but the loss magnitude, that is asset value into exposure factor, this we have already seen, this is loss magnitude. So essentially loss magnitude into, you annualize it based on number of occurrences in an year, you actually have an estimate of what is the loss magnitude over an year that is, that is what ALE is, annualized loss and once you have this figure, annualized loss expectancy, then you use that to calculate the cost benefit analysis or to do the cost benefit analysis. How do you do cost benefit analysis or overall gain or loss would be given by this formula, overall gain or loss, it can be a positive number, it can be a negative number. So you have seen what is the annualized loss expectancy so that you take, say an asset and know the loss magnitude and you annualize it and now you look at the current now, prior is before taking an action, so risk management experts have done already the risk assessment and there is currently a annualized loss expectancy and then the risk management guys propose that you invest in certain technologies, is the protection or mitigation or whatever.

So then post that investment, you expect a different ALE because now you have better protection or better systems in place. So annualized loss expectancy post investment, that is ALE post, this is ALE prior, this is ALE post. Now when you invest in a new system to improve your cyber security, you also incur a cost, that cost is annualized ACS. ACS is the cost for implementing the control, annualized cost of the safeguard, ACS. So what do you expect, which would be a higher term, ALE prior or ALE post,

whose value would be higher or should be higher? ALE post would be higher? It is about loss right, your, when your system is vulnerable, the losses are likely to be more.

So the current losses, expected losses are more because you are more vulnerable, your asset is more vulnerable. But now you invest ACS, you invest ACS to better safeguard your system and therefore you expect that the ALE, the loss will go down. Now the loss expected loss will be going down but you can see the trade-off that is coming in, in this part, ALE post plus ACS. So what justifies the investment in a technology for reducing the risk is ALE post plus ACS. This term should be less than ALE prior, then you have a gain, then it is a positive cash flow, then it is a gain, that is easy to understand right, this is nothing but cost benefit analysis.

So this term, so if what happens if ACS is very high, then actually it does not justify the control at all because your gain actually goes down. So reasonable investment in cybersecurity to improve your risk would justify that investment, if not it does not but you can see that all this economic analysis requires quantification and also monetize, expressing these terms in monetary values, okay and that is a separate effort but conceptually your investment should reduce the losses sufficiently to justify that investment, okay that is the rationale in this formula. And now we have seen risk assessment, then taking a particular control strategy, risk management strategy and then having, well gone ahead with the particular decision, it is important for the organization to continuously monitor because what you have at the time of an investment is an estimate of gains or losses, okay but actual can be very different. So the management also has to see that your investment is delivering the expected gains. So therefore, monitoring of the risk control strategies that you have put in place is the next effort.