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: 06
Lecture: 16

Good morning and welcome back to the sixth session of Cybersecurity and Privacy course and today we are going to cover Risk Management. So the risk management as a title looks like a very generic topic but in this session we are going to cover risk management pertaining to cyber assets or its cyber risk management that we are going to cover. So the management part of cybersecurity is the focus of this course and we saw that when we have to manage assets efficiently we need planning. So planning is the heart of management and we saw planning falls into two categories as far as cybersecurity is concerned. One is the contingency planning, which we discussed already and we also saw if there is no contingency planning procedures and structures in place what happens to organizations, they are struck and they have a shock and they are not prepared and there is huge losses and loss of reputation, loss of revenues and so on. And that actually calls for contingency planning as to how you respond to incidents.

So it is a reactive aspect of cybersecurity management. The other aspect of planning is planning to prevent occurrences of incidents. How do we prevent cybersecurity incidents? It is not about reacting to incidents but it is about preventing. So protecting the assets of the organization.

We also saw that in contingency planning, the analysis or the focus is business processes. Business processes get affected, when there are cybersecurity attacks. So the focus or the unit is actually business process. And today you will see that for the purpose of risk management the unit is going to be, not business processes but assets. It is assets that you need to protect.

So these are subtle differences between contingency planning and planning for risk management, risk management. All right. So let us move on I think. So yeah, so to introduce what is risk at a philosophical level we look at Sun Tzu. Sun Tzu is, of course, the military philosopher of China who lived 500 years before Christ and who continues to be a great influence not only for China but for strategy, military strategy.

And see the three classic statements that he makes. If you know the enemy and know yourself, you need not fear the result of a hundred battles. Well, there is a difference between what battle and war. If you know yourself but not the enemy, for every victory

gained you will also suffer a defeat. And if you know neither the enemy nor yourself, you will succumb in every battle.

So there are two things that are highlighted here, know the enemy. So who is going, who is, could be external, could be internal but in the case of cybersecurity. But there is an enemy, there is an enemy, okay and know yourself. So these are the two aspects, basically we are going to cover in risk management. Risk management is about what is the nature of threats that you have from the environment, internal and external.

And what is it that you have to protect yourself from this, the protect yourself from the enemy. Okay, so the word enemy actually makes a lot of sense. Somebody who is aiming to hurt you or to sort of create losses for your business and so on in the case of cybersecurity. So what is risk management? As I said it consists of two aspects, knowing yourself and knowing yourself is in the specific case of cybersecurity is knowing your assets. And knowing your preparation, your assets and your current preparedness to protect against the enemy.

That is the knowing yourself part. And knowing the enemy is the intelligence about the external threats that are potentially existing and could actually become an attack in future. So the threat versus internal assets and your preparation. So that is what actually we are going to cover in risk management. Essentially, risk management covers these two aspects.

So risk management is the process of identifying, assessing and reducing risk facing an organization. So there are three steps in risk management. First step is to identify. What do you identify? Basically in risk management you identify, what are your assets that needs to be protected. And you not only identify your assets, you also identify what are the threats.

The threats and the assets. And then how well prepared you are. So that is the assessment part. Identify them and then assess your preparedness or your assets protection mechanism, current protection mechanism. And then you will find as a result of this assessment process, you will find some gaps.

And how you close those gaps. And then there is a management decision as to how much you want to invest, what are the options available etc. That is about reducing risk. Look at the word used, it is about reducing risk. Sometimes you use the word mitigation.

There is a difference between reducing and mitigating. So these are nuanced

differences, we will see that. But the purpose of risk management is not to eliminate risk but to reduce risk. You have already told us in the world of internet, there is no 100 percent security. So if you use internet connected devices, there is no guarantee for tomorrow.

Alright, so that is what we are trying to do. Identifying, assessing and reducing risk. I think I used this diagram already to tell you threats, external as well as internal. And what is an attack? An attack is an incident that happens through some residual or some leftover vulnerability in the organization. And that is exploited and then it becomes an incident.

And therefore the chance of that happening is actually your risk or a proper assessment of what is the chance that a threat can become an attack and if that attack happens what is the impact. So a risk is an overall assessment of that. So we will see that in the coming discussion using different slides. Now today there is this term, attack surface which may figure in some literature, not in your textbook. So attack surface is a good visualization of threats and assets.

Threats and assets. If you see that there are two dimensions to an attack surface sometimes also known as attack vector. They use the term vector also, attack vector, attack surface also. So in talks, you can see people just keep using this kind of terms, sometimes without meaning what it means. Whenever you hear the term vector, you have to keep in mind that it is about a construct, something that consists of more than one item. You know the difference between a scalar and a vector.

Speed is a scalar because it is only about speed. It does not talk about direction but when you add direction, it becomes a vector because it is two dimensional. So in a similar way you can see in attack surface, you do not just talk about threat alone. Threat along with assets. It becomes more useful information.

So it becomes a vector. It has multiple dimensions to it. So the y axis is about the different types of threats that exist and the x axis or the horizontal axis is about the assets that your organization has. So every attack actually aims at some asset or some asset gets affected and as a result of the asset gets , getting affected certain business processes will get affected. So that is how this happens. So an attack vector, sorry an attack surface actually enables a manager to visualize what threats did materialize or did happen and what were the assets that were affected and in what sequence.

You can see the breach at Equifax is a case that we are going to discuss in a, after a few sessions. So you will understand how severe and how varied the attacks were in terms

of the different hacks that were used and which actually resulted in data breach not one or two, hundreds of millions of records of a credit bureau. Equifax is a credit bureau which actually stores the credit card and a lot of credentials of individuals which were stolen and that happened in 2017, not in 2000s when IT was evolving, a very recent, not very old case. So that shock, that is another big shocking incident in the cyber world and somebody has charted that attack surface in terms of the specific threats that happened with unpatched vulnerability, misconfiguration, these were issues but which were the assets that were affected correspondingly, that is what is shown here. Storage was affected or probably routers was affected.

So you can see what was the sort of target that the hackers used. So it actually plots it two dimensionally, known as attack surface. There is also the concept of residual risk before we go to risk management, we should be clear about what is risk and what is residual risk. Actually the purpose of risk management is to assess residual risk not actually risk because every organization, any sensible organization will have some mechanisms to protect its assets, at least there will be a security post, so that thieves do not come in. So there will be certain built-in mechanisms to protect or safeguard your assets.

So you can see in this bar graph, the bottom part is about amount of asset value protected by safeguards. So there is some basic protection that is available to every asset owned by a national or any organization which functions rationally. Look at Windows, as an example. So many of you may be Windows operating system users. So Windows operating systems come with certain basic protection.

There are built-in protection against vulnerabilities or against threats in a basic operating system. Even if you do not install a firewall or antivirus software you still have protection, built-in protection, that is the base. There is a base protection available and in addition to that you know, there so, threats are that are very dynamic in nature. So therefore in order to have more protection for your cyber assets you may choose to install an antivirus software or a firewall etc. So that is the second level, amount of threat reduced by safeguards additional safeguards that you put in.

That is your choice, how much you have invested in that. The third aspect that you can see in this diagram is amount of vulnerability. So after protecting your system using the basic base level protection and also additional protection that you give, there could still be gaps. Those gaps are known as vulnerabilities. So vulnerabilities is something that in cyber risk management, you act on.

That is for example, if you have not installed latest updates, Windows updates or

patches, you are vulnerable. That is a vulnerability, you can see that in many recent attacks the patches were not installed, particularly in Windows and that is the vulnerability that was exploited by hackers. So that is, but if you are updated, if you actually update your system regularly and consistently with security patches, then you are actually further reducing your risk. And even after these three levels of protection that you put in place there is still this much of risk and this is known as residual risk.

Residue means leftover. So there is some risk that is leftover, which is the residual risk. So the purpose of risk management, the first two stages, identifying and assessing risk essentially is about assessing residual risk. You have assets, you have certain protection mechanisms but what is the risk that is still existing, what is the residual risk ? That is what you try to assess in a systematic manner in risk management process.

All right. Now about risk management. So this diagram illustrates the different steps and phases, different phases and steps involved in risk management. So there are three phases one, two and three. Three phases in risk management. The first phase is risk identification. The second phase is risk assessment and third phase is risk control.

This is very logical -Identify, Assess and Manage or Control. So you cannot control unless you know, you cannot manage unless you measure. So that is a management principle. So therefore, the first phase in risk management is risk identification and what are the steps involved in risk identification. This diagram gives you a sense of that and that you can look at when you look at the different steps, you can see the first steps corresponds to assets, what do you have.

So that is about your assets, know what you have. So that is about your assets and also, you also look at threats and vulnerabilities. Identifying assets, identifying threats and vulnerabilities. So that is the specific exercise in risk identification. You identify each asset, cyber asset and identify the different threats that can actually impact the assets and also look at current protection mechanisms and have, so based on that identify vulnerabilities, identify existing vulnerabilities.

Risk assessment is the next phase and in that phase, you actually assess two important measures and those are very important in the calculation of residual risk. One is called loss frequency. The second is known as loss magnitude. Loss frequency and loss magnitude. Once you are able to measure and compute them or estimate them I do not say compute, you are able to estimate them, then you can calculate risk, here it is essentially, it is residual risk, calculate risk.

So in our discussion we are referring to residual risk as risk. So you will see that the

formula for risk has two components in it, loss frequency and loss magnitude. The effort in risk assessment process is to finally arrive at these two measures so that you can have a quantitative assessment. A quantitative assessment of residual risk using these two measures and you will see that loss frequency is related to probability. There are n threats in the world, does not mean that all the threats would materialize or all the threats are equally likely.

There is, there are probability scores associated with different risk. And also you have your own protection mechanism. So a threat has to occur by passing through our existing protection mechanism. So there is a likelihood of success also. So you can imagine that there are, it is probability driven.

The threat is something that is driven by probability that is what you look at here, when it comes to loss frequency. Loss magnitude is related to impact. Suppose an asset gets attacked, then what is the loss involved? What is the loss magnitude? And there are, so that loss magnitude can differ from asset to asset. There are certain assets which are high valued and there are certain assets which are low value. And therefore say, think of a e-commerce server, your company is purely running on running online and the e-commerce server, suppose it is hacked or by some reason, there is a cyber attack on it, your entire business stops.

So that value of that asset, it is not just about the cost of buying that asset but the value of that asset for business is very high. So as compared to maybe some office PC which is used for, you know, for much smaller scope of work, that its asset value need not, may not be very high or it may be low to medium. So therefore loss magnitude is also a function of the value of the asset. And then you can once you have these two parameters estimated, you can actually calculate risk and risk acceptability. How the organization wants to respond to this risk, residual risk is an organization's decision.

So therefore then, comes the risk control, select what are the options available how do you justify the selection of a particular option and in organization, there has to be financial justification. And how you do that and then, once you select a particular option then monitor it, monitor and continue to do the assessment. This is a dynamic process risk management is not something that stops at some point, it is not like strategic planning which you do for five years and then close it, this is a very dynamic process. And how dynamically it is being done, you know, you have to get feedback from different industry types. You have a guest talk from industry, so you may shoot many of these questions related to practice, to the person who is going to come in the next session and do not reserve any questions for me.

The first step is risk identification. Let us go through these steps and take some example to understand how you can actually quantitatively, assess risk, cyber risk. So risk identification is essentially knowing yourself in the, in terms of war strategy. What do you know about yourself? Basically your assets. So any sensible organization which is preparing to protect itself from cyber attacks should know what are the assets, the organization has. And if you have worked in professional organization, you know that every asset has a tag or a identifier.

Look at any asset. So I do not see any tag ID written on this but there will be an ID for every asset, not in educational institutions necessarily. But our department DOMS has asset tags and basically a tag is an identifier and along with that identifier, you will have the complete descriptive information about that particular asset. So identification is about knowing, what are the things that you have which needs to be protected. So you can identify them, give an ID and also have a database, that is the best way to keep asset information. And what are the different types of assets an organization can have, in the context of cyber assets ? That is what is shown in this particular table.

You can see that the assets fall into six categories. Are people assets? People are assets. Cyber bullying, Binod's research topic, probably evolving is actually an attack on an individual. So an individual is an asset, if an individual in an organization is attacked or bullied or if her or his information is stolen etc, this is nothing but a cyber attack on an individual. So people are assets, procedures are assets, your policy is an asset and your data, databases, they are assets. So organization should know what are the different databases you have.

Software, hardware, networking components, all of them are actually assets, asset categories. You can see these are asset categories and the table also describes what do they do, what do they, what is the functional aspect of each of these categories typically. So once, if you are doing this for the first time and if you are a small organization and you want to do cyber security management first effort is well, these are the categories, you have identify each asset and characterize them. So you can actually also gather descriptive information about your hardware, software and network assets, the hard and soft constituents of your IT system. And this depends also on the maturity of the IT, maturity of the organization.

And as I said every asset will have certain asset characteristics or attributes. So when you add an ID you know it is an you can imagine a database, so ID is like a primary key. So you look at a say a software, so a software, an operating system has an ID and then you can have different attributes of that particular asset stored in a database like the name, IP address if it is applicable, MAC address as a type, serial number,

manufacturer so on and so forth. These are typical characteristics of IT assets. So essentially we are talking about an asset database, asset identified, asset stored, asset information stored in a database in a structured way.

So physical hardware and software assets, it is intuitive but you also need to identify people procedures and data assets, people of course, the HR database, you have employee ID or a roll number etc. There are procedures which also need to be numbered, you know typically in a standard based system like the ISO, you have every procedure, will have a ID. So and, so that enables an organization to keep its assets systematically. Now yeah, so there are different types of assets for different asset categories that is what this slide illustrates. People will have different attributes, for example security clearance level, you know this is military language, what that means is what is the level of access or what is the authority, we talked about authorization, you know authentication and then authorization, what is the access level an individual has, okay.

Has an individual, for example in military setting access to confidential documents or secret documents or top secret documents, so this all is defined in the people asset identification stage. So therefore when you access a particular individual you know what is the level at which individual can access information, information assets. And you can see alongside people you also see data, so data is one asset which people access and therefore data also needs to be actually stored, data assets need to be stored with respect to its different characteristics, like who is the owner, creator and what is the size and where is it stored, is it online or offline and so on and so forth. And then like procedures, who is, what does the procedure do and what is the intended purpose, where is it stored and attributes like that. Now, here is an example of data classification because we are predominantly looking at cyber security from information security perspective, okay.

So in information security, data classification is a very important aspect, just like people are classified in terms of their authority, data is also classified in terms of its sensitivity. So data classification can be done differently for different types of organizations, okay. If it is a business organization, you may actually classify data as public for official use, sensitive, classified, this is an example, okay, four levels. And then of course, the clearance level is defined in terms of these four categories. We saw in people's case, they have a security clearance level, which is the level at which a person can operate, is in terms of these four classes.

And of course, US military has the most meticulous way of organizing data and you can see there is unclassified data, which anyone can access about military, sensitive but

unclassified data, someone from military should tell me what that means, but it is unclassified means it is accessible, yeah. Restricted, that is confidential data. Basically we have one which is we have security classification, unclassified data, there is a base classification. That is right. Then comes the restricted part which is basically restricted to few personal, yeah, few personal or limited people, then you come to the confidential, then the secret and then the top secret.

Yeah, so unclassified and sensitive are different in the sense, you restrict it to some extent, that is what they are saying. Confidential means it is confidential and access levels are very clearly defined. And secret data, it is about the number of people who can access, right and you know people at what level can access. Top secret of course, you know military has its own methods for defining and giving this kind of access, maybe the president or the prime minister or the commander in chief, so those are the type of people who have access to top secret in the military setting.

So people classification, asset classification is what we are looking at. There are different types of assets, right from hardware, software, people and data and they need to be classified, they need to be described in different terms. And the next important step as far as risk assessment is concerned, now you can see the term has changed from identification to assessing, okay. We are now trying to assess the value of each asset, okay. Because some assets may be very important or critical to run the business and some assets may not be critical, but important. So, as I said the assessment of an asset value is not based on the purchase value of it, but its impact on business.

So you can see generally for assessing value of asset, an instrument or a questionnaire is used. We can actually get expert information on what is the asset value. So typical questions in a, when you use an instrument for asset value assessment, is like, which information asset is the most critical to the success of the organization, which generates most revenue, which brings highest profitability, which is the most expensive to replace, which is the most expensive to protect, which will cause the highest liability, so on and so forth. So you can see, you can think of a scale, of say 1 to 5 in terms of the each item in this questionnaire, okay.

So that is what, how the asset value assessment is done. So here is an example, this is just taken from your textbook. So there are different assets which are already identified and classified and tagged. So one is this is, this pertains to a bit old generation, so they are talking about electronic data interchange, used in e-commerce. So EDI document set 1, EDI document set 2, you can see they are using three criteria for assessing the value of an asset. The three criteria are impact on revenue, impact on profitability, impact on public image.

That is what this organization does, okay. There are different questions you can ask, but based on these criteria, they actually arrive at a score, arrive at a score, a score between 1 and 100 for every asset. And each of these criteria has a weight. So it is a weighted score that you actually use to arrive at the value of an asset, okay. And you can see that there is one asset which is, whose value is 100 here, right, customer order via SSL. So that is the asset which hits a value of 100 because if customers cannot place order, your business stops there. Thank you.