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: 17

Alright, so now we have, we have looked at assets, we also have looked at the way to assess the value of assets. Now we are looking at the other category which is threats. So threats also need to be identified and threats also need to be assessed, okay, identification and assessment of threats. So how many cyber threats are there today? You can say many, okay, that may be better, a qualitative term there are many, okay. So but actually hundreds, okay. So I am not going to spend any time discussing each of the hundreds of threats that exist.

But there is something known as threat intelligence, okay. Threat intelligence actually is very informed information about what are the current threats, cyber threats and what is the criticality of each threat, which is the most likely threat, okay, which is the most frequent threat and which are the threats which have high impact etc. So this intelligence is something that is available, not with me, not in the textbook because it is dynamic but with professional bodies. So you talk to a practicing manager on cyber security, you will see, they have subscription to threat intelligence.

And the bodies which do this sort of analysis and data aggregation analysis and CERT, C-E-R-T to some extent is a body which provides this kind of information. But for more information, you need to have subscriptions or you need to have network with cyber intelligence bodies. And therefore that is the terrain we are entering now, as to what are the threats that exist and against which you need to protect your assets, you know, your textbook may talk about a few threats. But what I have done is, I have a more comprehensive list of cyber threats and their descriptions, to give you awareness about what are the different types of threats and which I will be posting in the module. So you go through them and some of the threats which are prevalent today, anyway we are discussing in along with case studies.

So you get to know about them more, okay. Alright, I think each of this would be discussed in some detail in the cases to follow. So I do not spend time on describing each threat at an item level or individual level. But threat, like asset are also classified. See when you have too many things, what you do? You classify, alright.

A manager needs to manage things efficiently. So you classify. Why there is product

segmentation in marketing or why there is customer segmentation? So you know, you cannot actually create product for each individual. You create generally product for customer segments. So therefore segmentation is the way to deal with complexity, or classification is the way to deal with complexity.

And here you can see again, threats can fall into say, 12 categories, 12 classes. So they are acts of human error or failure, compromises to intellectual property, deliberate acts of espionage or trespasses. What is espionage? Mike, Mike, okay. Espionage is an act by someone who is working from within inside the organization, against the organization. Yeah, yeah.

So this is basically someone who is or was a part of the organization or a country, actually betray the country or the organization by leaking out information. You have several cases of espionage related to US military. So we will touch upon that as we go. So espionage is a serious but higher level issue. So that is one category.

Information extortion where you actually try to threaten people and extort or get money or assets from people, that is another category. You can also see in this classification, the last one is technological obsolescence. Is that a threat? Technological obsolescence is classified as a threat category. If your machine is not updated, if you are having a Windows 8 and you are running your critical business on Windows 8 and you do not want to invest in software or hardware, you are running a high risk of cyber with respect to cyber security. And you have cases after cases where machines became vulnerable as they are not updated.

So that is a threat category. So you can see that threats fall into categories. So that is the way to understand. So when you look at each item or each threat, try to imagine which category of threat that is because that numbers are limited. And this is again drawn from a paper communications of the ACM where some scholars published information on threat severity or they try to rank the threats.

And you can see for ranking the threats, they have used a mean value that could be with respect to occurrence and their weight, the mean and the weight it is not clearly described here but you can see, there are aspects to the threat in terms of how severe it is going to be and what is the sort of likelihood or what is the frequency with which that particular threat is happening. And there is of course, a standard deviation which is calculated there. But to assess the weighted rank of a threat, they multiply the mean with the weight, the mean with the weight. We do not know how these weights are assigned but the mean value calculation is from data. So essentially this particular table tells us that in cyber intelligence for threat or in threat intelligence, you quantitatively

assess the threat.

There is a assessment, there is a value, there is a score that is given to each threat. And therefore, threats can be ranked or threats can be sorted based on the weighted rank of each threat. Some threats are not likely or they are not having any impact and therefore they get low value and some threats are highly likely and highly impactful and they get high scores So this score of threats are with intelligence bodies which needs to be available for cyber security management, particularly for the assessment of threat. This is not something that you can do internally. When we looked at assets and asset identification and valuation, this is something that you can do internally.

This is, assets are internal to your organization and its valuation is also internal. You can run a questionnaire survey and finally arrive at the valuation of assets. But threat intelligence, you do not have the data. This is external data. And therefore for threat intelligence, you will be dependent on external bodies.

So once you have assets and threats, you can now imagine there is one axis of assets and and another axis of threats, okay, threats and assets. And then there is a threat-asset combination. For each threat and asset, there is a combination. And that is where you ask this question, what is the vulnerability, as far as this threat and this asset is concerned. Now we have gotten into the micro detail of risk assessment at a threat asset level or asset threat level.

So vulnerability is something that you assess at each combination of asset and threat. When you consider these two together, what is the vulnerability. That is something that has to come from experts. Or that is something that has come from judgment. Are we fully protected? Is this asset protected from 1 to n threats and to what extent? Are there some leftover vulnerabilities or are we 100 percent?, okay.

So that is called vulnerability assessment. So you can see that between asset and threat, you know, it is shown in the diagram. Between an asset and threat, lies the vulnerability. A vulnerability is with respect to a given asset and a given threat. Now you will see how, this is an example, vulnerability assessment of a DMZ router, okay, but well this is a technical term, essentially a proxy system.

Now you have a real server, you have a proxy server. Proxy server just act as a shadow or a, you know, a copy of the real server. So that kind of a system, so they are taking a router from that zone and then assessing the potential vulnerabilities. So you can see that you took one particular asset and then you are going through each threat and describing what are the potential vulnerabilities. You get the point? Take one router

and all the threats, and then describe, what potential vulnerabilities exist.

That is the process of assessment of vulnerability. For every threat, this is done for every asset. Now I will take you to this important spreadsheet, which is used in risk assessment. So you can imagine this is a, this requires a spreadsheet, because this pertains to cell. There is a cell which pertains to two dimensions.

So each cell will actually chart the vulnerabilities. So threat vulnerability asset worksheet or so known as TVA worksheet, is the final tool. I will show you an example. And this is in your mind already, I believe. You have one axis which is for threats, you have the other axis which is for assets.

So as we said, so the DMZ router, so that is one asset. So you can see that assessment of the vulnerability is done for each threat. So the first column would list the different vulnerabilities for asset 1, with respect to different threats. So the TVA spreadsheet is a tool or an instrument used to assess vulnerabilities in a detailed way, for all threats and all assets. Once you have this in place, you have a fairly good assessment of what are the vulnerabilities, the organization has.

And you also know that you can rank order the assets and rank order the threats here, because you have the asset valuation done. So therefore you can rank order them. The threat intelligence you have and therefore you can rank order them. So therefore the top ones or the first diagonal can be the most critical in terms of the vulnerabilities, okay. So that also helps you to look at threats, the vulnerabilities in terms of their criticalities, alright.

So that is the TVA spreadsheet. And in the world of practice, TVA spreadsheet is a very important instrument for vulnerability assessment, okay. So when you hear the word vulnerability in cyber security, always keep in mind it is with respect to a particular threat and a particular asset or a vulnerability. What is vulnerable? We say I am vulnerable, right. Because you feel very vulnerable. So I have an asset, as an asset I am vulnerable with respect to 1, 2, 3, 4, N threats.

So therefore keep that perspective in mind. Now having done or having prepared your TVA worksheet, you are inching towards the next step of quantitatively assessing risk or doing the risk assessment in numbers. So there are two terms as we saw in the beginning, loss frequency and loss magnitude. These are the two terms that are used to calculate risk. So what is loss frequency? Loss frequency is an assessment of the likelihood of an attack combined with expected probability of success.

So there are two probabilities here in a sense. One is how likely an attack can happen, okay. A DDOA versus a phishing attack, which is more likely today, that is an external intelligence. So what is the probability of that attack versus if that attack happens, what is the chance of success, okay. An attack can happen but you are fully prepared, with your malware protection or with your firewalls updated.

So if you do not have a firewall or if you do not have updated security systems, your vulnerability or your chance is high, okay. So that is what you do during the vulnerability assessment. So these two probabilities together, well you can imagine to get this, you need to have those probability values, somebody need to tell us, okay. You need to have this data. Otherwise it becomes qualitative assessment.

So in quantitative assessment, you need to have access to data to arrive at these two probabilities, likelihood of attack and likelihood of success. These two together defines loss frequency. It is, it assigns a numeric value. Use external references of values, of course we discussed this already. So it is a probability which combines attack likelihood and success probability.

The second is the loss magnitude, loss frequency and loss magnitude, standard terms in risk assessment, risk computation. Loss magnitude sometimes is referred to as asset exposure. This term exposure is sometimes used, right. Exposure is well, you have an asset and there is a particular attack possible. But the asset may not be completely exposed, okay.

Part of the asset may get exposed. So if it is 100 percent exposed then it is the loss magnitude is high but if it is not, then it is proportionate to the exposure. So what is this particular value? It combines the value of information asset with the percentage of asset lost in the event of a successful attack. So if an attack happens, what percentage of that asset is stalled or impacted is the basis, for measuring loss magnitude. So there is a asset value multiplied by the percentage of asset affected during an attack.

So the product is the loss magnitude. We will take an example as we go and then you will understand this a little better. Well, here is the magical formula for calculating residual risk. Residual risk, okay, I have not used Greek letters, it is actually more textually described so that you very well understand what it is. Loss frequency times or loss frequency into loss magnitude minus So loss frequency into loss magnitude minus the percentage of risk mitigated by current controls plus measurement uncertainty. There are 4 constituents in the calculation of residual risk.

Loss frequency into loss magnitude. Typically you will think that this is risk but it does

not stop there. So probability into impact, usually risk is described as that, what is the probability of something going wrong into what is the impact. Usually you describe risk as that but you can see, this is a more detailed formula that is one aspect of risk, loss frequency into loss magnitude or probability into impact minus the percentage of risk mitigated by current controls . There are certain current controls in place that is mitigating some of those risks, so you minus that.

But then you add a measurement uncertainty. So we have to keep in mind that the loss frequency and loss magnitude are estimates. These are not objective, this is not objective assessment, this is often subjective assessment and therefore there can be errors and that is called measurement uncertainty. So you add that and uncertainty as a value is added, you know, so that you know you are looking at risk, so you always be prepared for the worst, okay. So we are actually adding a worst case to the risk that is calculated using loss frequency, loss magnitude and the current controls. Alright, I think you just keep this formula in mind and then let me give you a problem and try to calculate the residual risk, this is the question, okay.

Well, I give you 3 minutes, just try to work out the, calculate the residual risk. An e-commerce database has 10% chance of an attack this year based on industry reports, that is one attack in 10 years. InfoSec department reports if the infrastructure is attacked there is a 50% chance of success, based on current asset vulnerabilities. So they have calculated vulnerabilities quantitatively. So if that particular attack happens, there is a 50% chance of success.

So you got the two probabilities there and the asset is valued at 50, that is a scale, in a scale of 0 to 100 and InfoSec informs that 80% asset will be compromised by a successful attack. So you have the exposure there. So these are 75% accurate, estimate risk.

You forgot the formula. You can note it down. LF into LM minus current controls plus measurement uncertainty. So basically you have to calculate loss frequency, loss magnitude, current controls and measurement uncertainty. These are the 4 values you need to calculate residual risk. What is loss frequency? Loss frequency is a product of chance of attack into probability of success. So therefore chance of an attack is 10% means in probability terms, this is 0.

1, correct. And what is, yeah, so chance of success is 0.5, right, 50% at that. Anyone got the final value? No? Okay, this is 0.05, agreed, okay, we will go. Loss magnitude is the exposure, right. So the asset is valued at 50, okay, 50 is the value of the asset into what percentage of it is exposed, 80%, okay.

So therefore 0.8 is equal to, correct, 40, 40, exposure is 40. Now current controls, is it mentioned? It is not mentioned in the question, okay. So therefore we just do not add any value there. So then measurement uncertainty, there is an uncertainty of measurement. So yeah, so you have to, you are going to calculate risk as probability to impact LF into LM, right.

So LF into LM, LM is equal to 0.05 into 40 means how much? 2. Now there is no current control. So essentially this particular estimate of 2, has a uncertainty. What is that uncertainty? It is only 75% accurate, meaning it is 25%, there is 25% error, okay.

So the 2 has a chance of 25% error. So error is equal to 25%. So measurement uncertainty is that error into the value which is estimated, right, which is equal to, measurement uncertainty. Measurement uncertainty is 0.25 into 2, that makes it 0.

5. Therefore residual risk is equal to 2 plus 0.5, is equal to 2.5, okay. This is a textbook problem solving. LF into LM is 2, loss magnitude into loss frequency is one aspect of risk. That is what you estimate based on asset value, threat, estimate, etc.

Each of these are prone to error, these estimates are prone to error. So when I calculated this value 2, it is an approximation, it is an estimate and that has some error which also they have actually, you know, this is a textbook problem, okay. So they have some assessment of it. So I am calculating measurement uncertainty as a worst case. Because of this inaccurate assessment of LF and LM, my value of 2 may be underrepresented.

So I want to actually add that 0.5 as measurement uncertainty to increase the value of risk, essentially saying it is not just 2, I am a bit uncertain about this 2, okay. So 0.5 is added by calculating error into that value 2. Yeah. Okay, so I will stop here because we need to have the case discussion and I have overshot a bit.

And here it is worked out and this problem is of course, very simplistic and actual estimation of these value quantitatively would be a challenge and you can see in real world, you can ask the practitioner next week as to how they do the TVA sheet, to what extent are they able to objectively assess these values and calculate risk quantitatively. Often times, we can see this is done qualitatively than quantitatively because of the difficulty of getting the exact quantitative estimates, okay. The risk mitigation or the risk management, now having got these values and for different assets, what action the organization should take in terms of controls and monitoring is the next step, okay, the third phase which we will discuss in the next class.