Practical Cyber Security for Cyber Security Practitioners

Prof. Sandeep Kumar Shukla

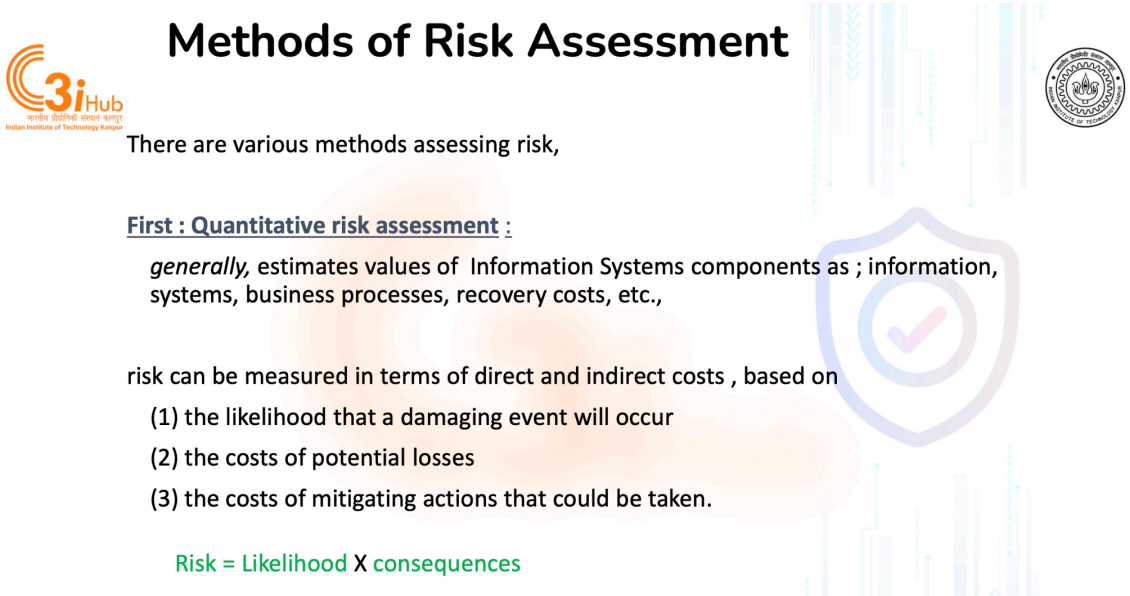
Department of Computer Science and Engineering

Indian Institute of Technology, Kanpur

Lecture 19

Deep dive into Risk Assessment-I

So, as we discussed, you have to understand what threats are now possible in your system and then what are the vulnerabilities in your system. And then you have to figure out what are the likelihoods for the various threats to be realized in your system through the vulnerabilities and then you have to figure out the impact of those threats being realized and this we already talked about. that budget is limited and therefore, we have to basically risk is not an absolute quantification of risk, but relative quantification of risk. That is whether some asset is at more higher risk than another asset that relativism is more important than exactly exact quantification of the risk. and again the risk is not fixed or static it is dynamic as threats change the threat landscape evolves new vulnerabilities come up new ways of attacking systems come up. So, we get more more likelihood the likelihood changes and sometimes the impact also changes based on the business conditions business priorities change right.



So, all these things are dynamic and therefore, it has to happen in a cyclic fashion that I have to have risk assessment every so often, like maybe 6 every 6 months. Also when some significant changes occur for example, some new assets are added to the system

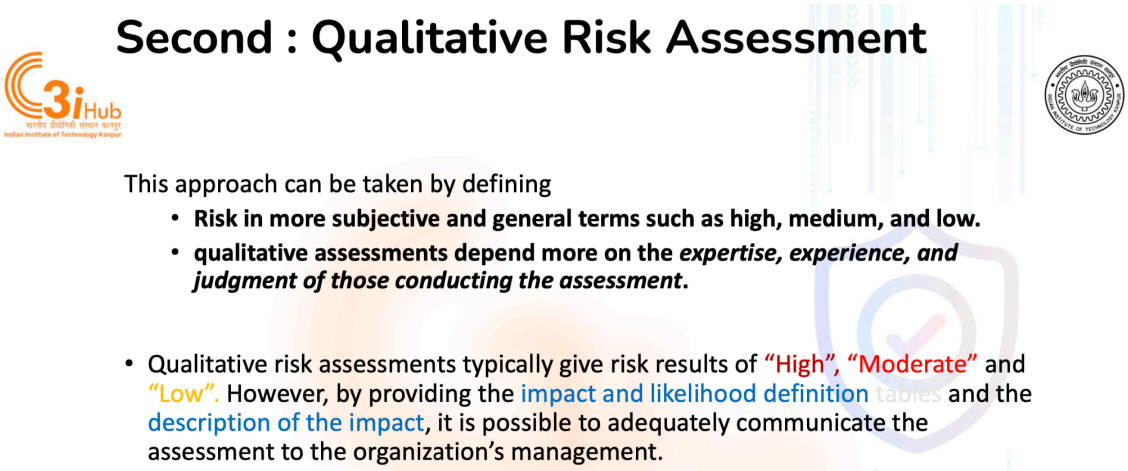
new business processes are done like earlier. Maybe you were not doing business by taking UPI payments now you have added UPI payments based business. So, that is a change in business process or new addition to the business process. So, you have to figure out what risk you know and what changes that you need to consider in terms of your risks to various assets involved in your various business processes.

So, the risk also is a decision making tool. So, because you have to decide what kind of cyber security you want to provide for various assets. based on the risks they are facing. So, there could be different ways of doing risk assessment. So, one is obviously a quantitative method.

So, in quantitative risk assessment you actually get a number for a risk right. So, you actually compute the likelihood of a particular event happening and then you multiply that with the damage or consequences that you have to incur in case that damage happens that will give you an expected consequence or expected loss. So, think in terms of life insurance when you buy life insurance. Let us say in that case there is only one threat to the insurance company right. The threat is that it has to pay out in case you die before the maturity of the life insurance they have to pay out right. So, they have to compute the risk and if the risk is acceptable to them then only they will sell you the policy otherwise they will not.

And how are they going to compute the risk? They are going to say what is the likelihood that this guy will die before the maturity date right. Now, how do you compute what is the probability of the person dying? In this case they have data from hundreds of years at least 100, 150 years as long as insurance businesses have been around. They have data about the people you know with what kind of health conditions, what kind of ethnicity, what kind of family history of disease, what kind of jobs function they are in etc. So, they have a huge database right. So, using that database they can actually compute the probability of a person dying below the age of X.

and then at that time the payout that the insurance company has to do would be the risk to the insurance company. So, if the probability of somebody dying is very very small, then at that time the payout may be very small, so then it is acceptable. If it is if the person is at a high risk category for example, the person is diabetic, the person has a smoking habit, obese and has a family history of heart conditions and all that stuff, then the probability from that data that they have. So, from that they will do statistical prediction and then they will say the probability is 0.8 and then I have a very high payout.

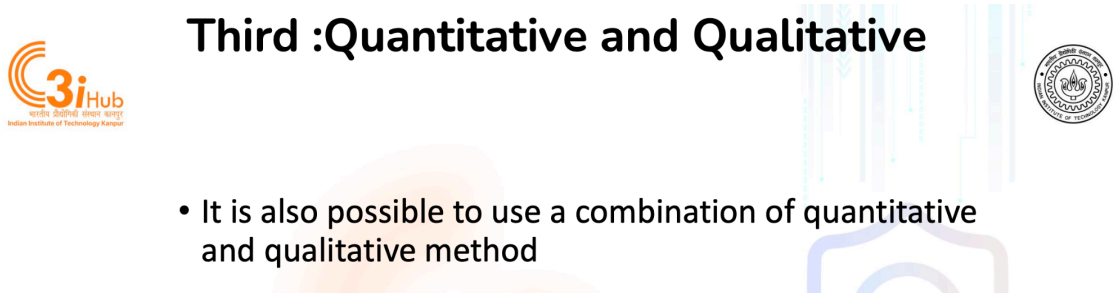


So, I am not going to intrude on this person right. So, this is what is called actuarial science right. So, there are actuarialists who actually do this kind of risk calculation. So, quantitative risk assessment is common in the field of insurance, car insurance, health insurance and life insurance and so on, property insurance. However, in the case of cyber, it is very difficult to actually do the probability calculation because we do not have hundreds of data of various kinds of attacks.

right we do not have the right set of features. Let us say I have IIT Kanpur and IIT Delhi and you have an attack in IIT Delhi system that does not give me much information whether IIT Kanpur has the same exposure right because they might have a completely different system, they might be using a different companies firewall, they might have a better or worse set of system administrators who configured the firewalls, they might have a different way of blacklisting IP addresses, they have all kinds of differences might be there. So, from the one I cannot say the exact probability of the attack. So, even if I see 10 different institutes getting attacked by similar institutes, I cannot really pinpoint the exact probability that my organization will also have the same attack. However, I can qualitatively say that if that is happening, if all institutes in India suddenly get a lot of attacks, I will then rate my chance of getting attacked at high right.

So, I can do a qualitative estimation of the likelihood, but I cannot do a quantitative estimation of the likelihood. So, I can say at this time this threat like a DDoS threat at this time may be high or low or medium depending on. what is happening around in the threat landscape also in terms of what is my exposure, what kind of vulnerabilities I have with respect to DDoS attacks right. So, if I have public facing internet services which can be communicated to through HTTP messages or through by pinging or through TCP handshaking connections and I do not have. DDoS, anti DDoS, DDoS protection filtering I might have I might rate the possibility of a DDoS attack tomorrow as high.

If I have the right set of tools in place, cloud flare or some other anti DDoS protection, frontend for all kinds of internet facing services I might say that it is a medium or low right. So, I can do these kinds of estimates in a qualitative way. So, when I do the likelihood estimation in a qualitative way then impact calculation also has to be done in a qualitative way right. So, I cannot multiply the qualitative terms like high, low and medium with a number right. So, I have to also say ok.



So, the likelihood is high and the impact is low. So, I might decide that basically makes my risk as low or I can create a matrix where I have likelihood high medium low and I have on the columns I have the impacts high medium low and then each cell will basically say what is the risk. So, for the low risk, sorry low likelihood and low impact, I will put the risk as low, but for high impact and high likelihood I will put the risk as high and then I have to decide what I want to do, whatever how I want to create the metric size. So we will see more about that, but this is the most common way of doing risk assessment in the cyber security field because we do not have enough data like we have in the life insurance or insurance business. we might have a qualitative quantitative combination.

So, we will see what that means in an example. So, sometimes I have quantitative data, but my likelihood is computed in a qualitative way, but for impact I have real quantitative data. then I made create thresholding, I say ok if the impact is thousand dollars, I sorry thousand hundred thousand dollars above hundred thousand dollar I will call it high. If it is built between fifty thousand and hundred thousand dollars I will call it medium and below fifty thousand I will call it low. So, I can actually convert the quantitative data into qualitative to match the other part, that is the likelihood data that is already available in the qualitative manner.

Difference in Risk Assessment for Insurance vs Information Systems

- Quantitative risk measurement is the standard way of measuring risk in many fields, such as insurance,
  - but it is not commonly used to measure risk in information systems.
- Two of the reasons claimed for this are
  - 1) the difficulties in identifying and assigning a value of all components
  - 2) Moral Effects couldn't be measured by quantitative measurements
  - 2) the lack of statistical information that would make it possible to determine frequency.

- *Thus, most of the risk assessment tools that are used today for information systems are measurements of qualitative risk.*

So I already discussed this that in case of insurance you can have the different measurements you have many years 100 years of data. So you have statistical information and it is also the fact that certain things cannot be always measured in terms of numbers right. So, let us say you are a power generating station and an attack causes an explosion. and the explosion either injures or kills people right. So, in 2018 or 17 there was an explosion of a boiler in UP in one of the thermal power stations where almost 60 people were killed.

Now that was not a cyber attack at least as far as we know as of their version of events, but something went wrong right. So, not necessarily all industrial accidents are cyber induced. It could be an actual accident also, but in any case if you want to compute the impact of such an incident right. Now the impact of such an incident cannot be done in a quantitative way. right because how are you going to measure the loss of life in terms of money. Now one way a company can decide to do this is by saying that there is a compensation I have to give to the person who dies to his family right.

Let us say I have to pay 5 lakhs per death per dead person. Let us say that is how politicians do that right when a train accident happens they declare that every dead person gets 5 lakhs and the injured person gets 1 lakh or something right. So, you can actually do that and then you can measure that as an impact right, because to the company's bottom line that is what it is right 5 lakhs per person 60 people dead. So, 3 crores is the bottom line that is the impact right, but that has a moral hazard right. How are you going to quantify people's death like that right? So, most of the time we do not quantify in numbers.

So, we say if even if one person dies it is a high impact right 60 though is very high very

high impact. Even if one person gets injured it is a high impact right because you should not have people injured right. So that is why we actually have a fundamental difference because in the insurance industry when people die. already his death has been quantified while taking out the policy right while taking out the policy we said that if he dies his family will get so much 50 lakhs or 1 crore whatever. So it has already been quantified so there is no moral hazard there.

But here there will be a moral hazard so that is why we do not do risk in terms of numbers in many of these cases. So now the question is how you are going to know the exact steps that you have to follow to compute the risk. So here you have to basically it is like the staircases. So you have to first identify the threats. Now this is a difficult one especially for newcomers you know because you have to understand whenever you look at a system.

So, you look at Pingala right right. So, when you say ok. So, I use Pingala. What are the threats that could have affected Pingala right? So, what would you know, you look at Pingla and you say ok what do I use it for, I use it for registration, I use it for leave application, I use it for you know grades right. What else do you use for right payments right?

So, yeah so let us say these are the 4 business processes that concern you in Pingla. Now you have to think about what can go wrong right. So, one thing is that you know that this is sitting on a database of everybody, all students right. So, data exfiltration is obviously a big threat right now. So, data exfiltration is a possibility, second possibility is that somebody can, somebody can get into pingala's in with a high privilege by exploiting some vulnerability and changing some data they change your grades right.

So, it can be either done for better grades or for worse grades right depending on who is doing the changes right. You can also think about doing an attack during crucial times like registration time, right. You do a DDoS attack on Pingala, so people cannot register. So, this way there is a whole process of threat modeling right. So, this is what threat modeling is about.

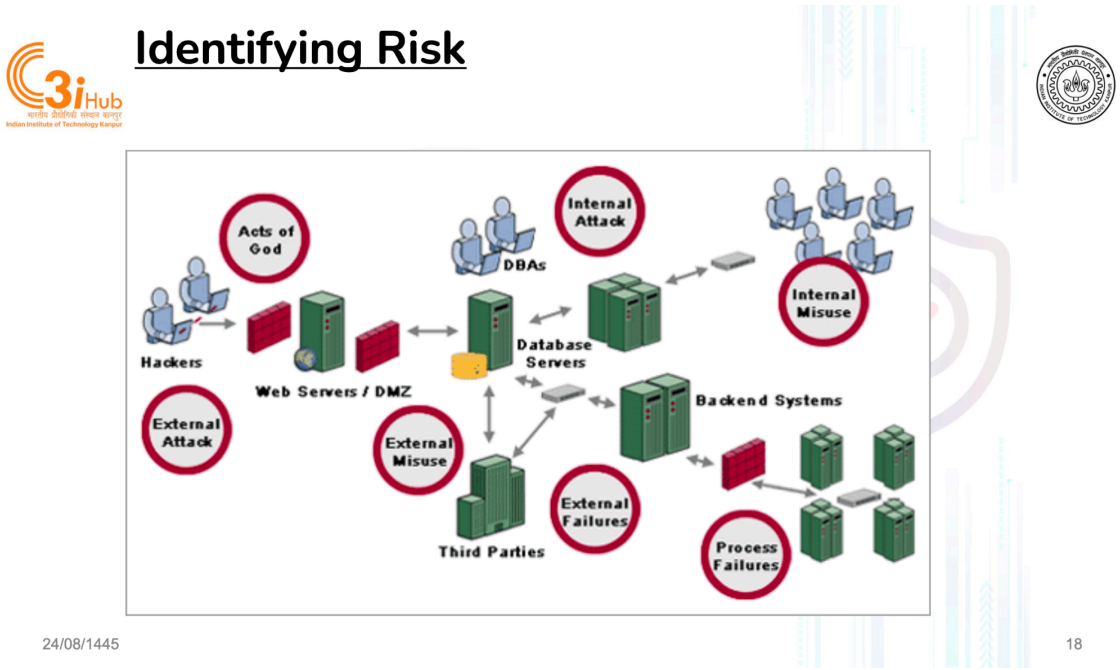
You have to imagine what are the different things that an attacker would like to do. It could be an inside attacker insider attack or it could be an external attacker, but this is what threat modeling is all about. So, you have to identify the threats. Now you have to see whether these threats are doable or not right. So, because data exfiltration may be a threat, the security of Pingala may be so good that you do not have a way to do data exfiltration right.

There is no way to do an account takeover, there is no way to do privilege escalation, there is no SQL injection and there is no way for external people outside the campus to access Pingla, let us say, because it requires a digital certificate at your browser. I am just saying it is not the case with Pingala, but I am just saying that you could have done a lot of things to actually tighten the security of. what we call hardening right. So hardening the security of Pingala. So in that case you will say that ok the data exfiltration threat the likelihood is close to 0.

There may be some unknown ways it can be done, but as far as I can see all the vulnerabilities I have checked I do not see that very likely. So I will put the likelihood to be low. On the other hand DDoS you might say ok so the login page itself does not have a rate limit right. So I can do a DDoS attack right. So you might say ok so, DDoS attack that vulnerability is there that vulnerability that will actually make the DDoS work is there.

So I will put the probability of DDoS as high. So and then you might consider another threat and then say can there be a data integrity violation, can somebody get in and change the CPI or change the grades. So you will look for vulnerabilities and then you will find that there is a way to actually do something like become the administrator and then you know how to get in. I am just guessing there probably is not is not any such vulnerability. But so this is the process of relating the threats to the vulnerability. So you start with four different threats that are likely and then you look at all the vulnerabilities to do that you have to find the vulnerabilities and then you relate each threat with each vulnerability and see if that threat can happen by that vulnerability, by exploiting that vulnerability.

Now then you determine the likelihood right, so you say ok so this is possible, but this is very unlikely and things like that so you will get the likelihood. And then you have to evaluate the impact for each threat right. So, what would happen, what would be the loss if there is a data exfiltration, what would be the loss if there is a data integrity violation, what would be the loss if there is a DDoS attack, what would be the loss if there is unauthorized access. So, you have to compute the impacts. And then you have to work with these two things: likelihood and impact for every asset in your organization.



So here just an example system you see that there is an organization in the organization there are regular users on the very corner. at the right hand upper upper right hand corner there are some people you know working inside the organization. The organization has database servers, back end systems and various internal systems which are segmented from each other. So, you see a firewall. The red firewall segments this part of the network from the on the right hand side part of the network from the middle part which says back end system and database servers and so on. And then you have the web server which is in a separate part segment of the network and you see another firewall that is a different segment of the network that is a demilitarized zone or DMZ.

And then you have another firewall to the DMZ and this is where the web server, the web server sits in the DMZ and external people are going to connect to the system through the web server. So, a web server is one conduit from outside to inside the organization, another conduit is the third parties. So, there may be vendors and all. who are connected to the organization into the system like for example, you can have a vendor you do not have enough IT people to configure your servers. So, you have a vendor who supplies the server and also connects to your system through maybe VPN or SSH or

whatever to actually configure it right.

So, that is what the third party is all about. Third party connects system through this router you see that there is a router into your system. So, we often, especially this is true in India, that often people allow third parties to configure patches to upgrade systems from their organization into the internal system. So, having understood this structure of this entire organization, this simplified simple organization, if we have to think about what can go wrong, where there are cyber risks, where at the cyber risks. So, first of all acts of god, we cannot do anything about there could be a power blackout. So, see eventually, one thing you have to understand is that when we talk about risk, we talk about the businesses bottom line right.

Risk is always about money even though there are some moral hazards about thinking only about money, but risk is all about money. So, where can a company suffer loss from cyber for any kind of risk? When its business processes are interrupted, its business processes might include things like they might be a supply chain company, they might be an e-commerce company, they might be a government service, they might be an industry like a power generation, power transmission industry, whatever. The organization's business processes depend on many cyber assets, servers, databases, network equipment and all that stuff right. So, anytime your business process can be interrupted anything that can create an interruption for your business process any of the business processes.

will be considered a source of risk right. So, the act of God is obviously a source of risk which is not exactly a cyber risk, but it can affect cyber. For example, if there is a flood that floods your data center right and all your servers are in the data center and all the all your services are running from your data center right. Now there is a flood in your data center. All the servers you know are totally out of commission and you have your business which cannot run. Nowadays most organizations have what they call a DR site. So, they have a data center primary data center or PDC and then they have a DRC, disaster recovery center right.

So, whenever there is a flood or something, exact replicas of all services are running to other data centers. So they switch over to the other data center right and this other data center usually is in a different geography than this data center. So most financial institutes if they have a data center in Bombay, their other data center is in Hyderabad or Bangalore or even Noida or Gurgaon or someplace right because if there is a flood in Bombay it is unlikely that there will be simultaneous flood in Gurgaon or Noida or something. And then you may have a third data center which is a disaster disaster recovery center right this is the second level. If both the primary and secondary fall apart then the third one can take over. So, depending on the criticality of the business if the business is for example,

Bombay Stock Exchange or National Stock Exchange.

they have to have guarantee continuity of service irrespective of weather or whatever right. So, they have to have at least primary, secondary and what do you call a data far recovery site or third recovery site. But in any case so that is act of God is one such thing. But the other one is hackers right, so hackers can come and start to figure out they do reconnaissance, they will try to figure out if there are weaknesses, vulnerabilities on your front end of your web applications or any other network facing internet facing services and they will try to exploit. Now, so these are the hackers will part of external attacks right.

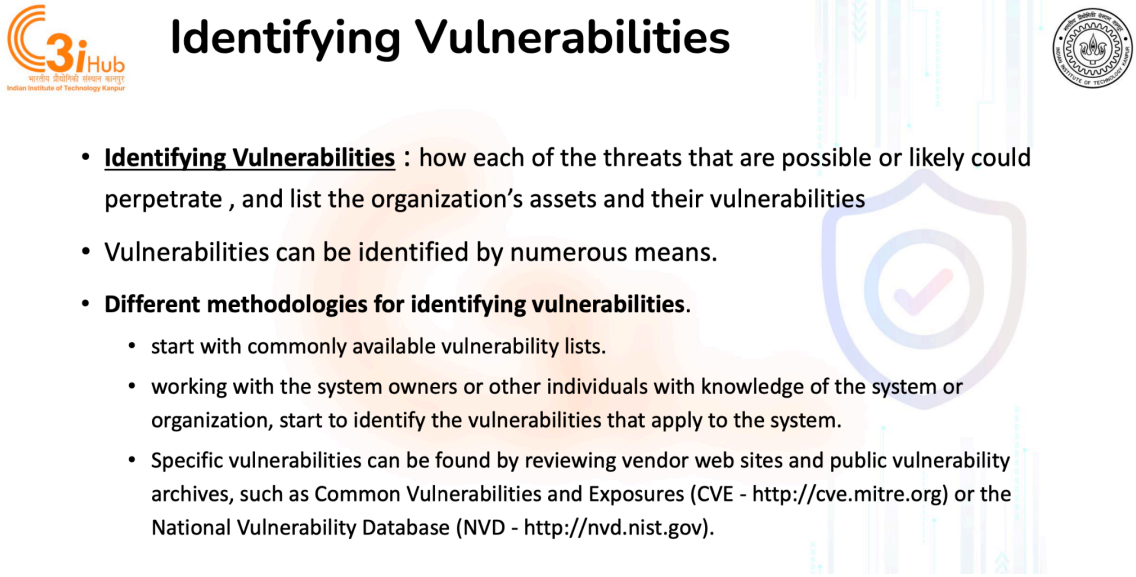
Then you have the third parties having connection and ability to access your servers or your network because you allowed them to do so because you have a trust relation with them right. You never know that one of their guys could actually misuse it. They can misuse this given access. So, that is why it is called a misuse not an attack because it is a you only you only gave them the access they are just going to misuse it in order to exploit your system.

Now there could be internal attackers. or internal misuse right. So people who have access to the critical resources might misuse the access or people might actually who are not given access but they are internal to your system they might try to hack into those resources which they do not have access to. Understand the difference between misuse and attack. The attack is when you have not given them the access but they force their way to get access that is an attack. And if you have given access and they are misusing it to exfiltrate data or to misuse in some other way then that is a misuse.

So you may have this internal attack and internal misuse and then you can have obvious process failures you know you can have. the third party failures or the process failures. So, this is just to give you an example about how to go about thinking when you do risk assessment right. So, when you go into an organization and you are asked to do a risk assessment, you have to understand their business processes correctly and then you have to understand which assets are involved in which business processes. Then you have to think in terms of threats to the business process and then translate those threats to that business process.

into threats to assets right because if I want to let us say you know do a data exfiltration from this database right. So, then I have to at least access the database server and then I may have different paths to the database server one is through the web application one could be through the third party one could be through the insider. So, you have to enumerate all those to figure out what their threats are. So once you have gotten an idea

about I mean once you have enumerated all the threats then you have to identify vulnerabilities right. The vulnerabilities could be hardware vulnerabilities in the hardware like there are some known vulnerabilities in the hardware, it could be in the firmware, it could be in the software, it could be in the networking network stack, it could be in the operating system, it could be in the application or it could be in the system architecture and it could be also in the business process right.



So, an example of a business process. In 2008, the vice-presidential candidate in the US presidential election was Sarah Palin and her Google account was hacked, right? And the way the Google account got hacked is, sorry not Google, Yahoo account at that time. Yahoo's account got hacked and so her Yahoo emails got leaked. Obviously at that time there was no two factor authentication, but the way it got leaked is because at that time Yahoo allowed it.

So, suppose I forgot my password right away. So, how do I reset my password today? when I go to yahoo and I say I have forgotten my password. So, yahoo will say ok. So, here is a fraction of your phone number starting with star star star whatever 0 4. I am going to send you a link there or some OTP there whatever right or it will say that star star star so and so ac dot in is your email address alternate email address.

So, I am going to send you a link to that email address. But in those days you could actually reset your Yahoo email by answering some questions and answering those questions were based on data that you already gave to Yahoo. For example, what was the name of your high school? What was your mother's maiden name? Now Sarah Palin was at that time the governor of Alaska plus vice presidential candidate. How hard it is to do open source intelligence to find her high school name or her mother's maiden name right. So somebody got her a password reset.

Once you reset the password you entered the email right. So and then you can change the password then she cannot get into the yahoo account right. So, this is a business process fault right. So, this is not a vulnerability in the software or operating system or application. Yahoo's process of resetting the password was at fault right. There was another interesting case where Yahoo, one guy, one celebrity, his Google Gmail password was hacked.

Now this is more interesting than Sarah Palin's case because what happened is that when and this is some time ago now this thing is not possible. Google and others have fixed it. So, what happened is that this guy, I think his name was Matt, somebody . He was probably a small - time celebrity, but people knew him. So, his Gmail account, so when some attacker tried to reset his gmail password, gmail helpfully said that here is your alternative email address, some mac dot in some apple apple email address where I am sending the alternative the link to reset your password right.

Now the hacker said ok so mac.in I let me see if I can get there right. So when he went to that guy's mac.in email address to try to reset it then it said that he would give me the credit card associated with your apple.com domain because Apple also has iTunes right. So you usually have a credit card associated.

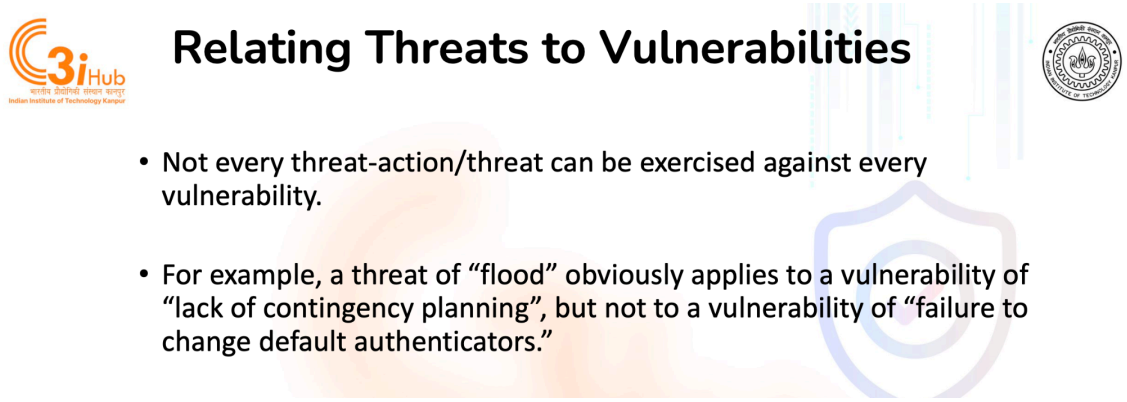
So then the hacker said okay so how can I get the credit card information right. So then he goes to Amazon, Amazon at that time to say Amazon you register a number of credit cards right to pay for Amazon products. At that time Amazon allowed you to add additional credit cards without logging into Amazon. So you can just go to Amazon, give your email address and say here is a new credit card I want to register right. So he registers this new credit card and then he tries to reset the Amazon password.

Amazon says give me the last 4 digits of the credit card registered with Amazon. Now he himself, the attacker registered that credit card. So he knew the last 4 digits. So he uses that and gets into the Amazon account. find another credit card of Matt right which was associated with that account which is really Matt's credit card and then goes to the Apple account and uses that credit card and lo and behold that is the credit card in Apple account as well. So, Apple account opens up then the reset link for Google came up and then he just reset the Google account.

So, here three different companies' business processes were at fault. So, individually each of them may not be at fault because Google was doing the right thing by sending the reset link to a different email address, but this Apple was doing the right thing by asking for some information that is very personal to that user. Unfortunately Amazon screwed

up, Amazon said that I can add an additional credit card and I can use that additional credit card to unlock your account. So, Amazon kept the door wide open right and from that there is a chain reaction. So, business processes are often at fault. So, it is not always that the software has some buffer overflow vulnerability or web application has a SQL injection or XSS or CSRF vulnerability it could end up in a process.

So, you have to think about business processes very well to know what kind of vulnerabilities they might have. But in any case the most common way to find vulnerabilities is to find the vulnerabilities in the hardware and software and that is what the CVE or NVD database is for. So the NVD database is where you find the known vulnerabilities for existing systems. So that is how you find the vulnerabilities.



Now not every threat and vulnerability pair makes sense right. So see there may be a buffer overflow vulnerability in an application and you are talking about a different threat that has nothing to do with exploiting a buffer overflow right. So maybe the data you know, well buffer overflow is actually a pretty generic one. So, it can be exploited to do a lot of things, but you may not have every threat vulnerability pair making any sense. So, in that case the likelihood is basically right. So, whether a particular threat can be exercised by exploiting a particular vulnerability has to be considered.

And, based on your knowledge of vulnerabilities, how they can be exploited etc., you can determine whether the likelihood is right. So, here there is an example like vulnerability of flood threat of flood cannot be affecting failure to change default authenticator. So, even buffer overflow may not be exploited to consider the you know flood or unauthorized access or something. Unauthorized access can be actually realized by buffer overflow.

Defining Likelihood

Likelihood is :

- the estimation of the probability that a threat will succeed in achieving an undesirable event
- is the overall rating - often a numerical value on a defined scale (such as 0.1 – 1.0) - of the probability that a specific vulnerability will be exploited

- **Sample Likelihood Definitions**

	Definition
Low	0-25% chance of successful exercise of threat during a one-year period
Moderate	26-75% chance of successful exercise of threat during a one-year period
High	76-100% chance of successful exercise of threat during a one-year period

21

So, now comes the way you want to define the likelihood. So likelihood is basically the probability right, that given this vulnerability what is the probability that this threat can happen right. So, for every vulnerability, every threat, this pair you have to consider. Now for certain threat vulnerability pairs it would be 0 you know by just looking at it you can say it is 0, but for others you have to consider whether it is possible to exploit that vulnerability to make that threat possible. And based on that you can actually decide that I will use low as so as I said it is not easy to give a numeric score to this right because we do not have enough statistical cases that will tell us you know what is the exact possibility you know to get this right. So, for example, many of you have taken statistics class and you know about sample proportion right.

So, sample proportion is an estimation of the population proportion right. So, an unbiased estimate of population proportion you might consider, you know, if you have enough samples you could have probably computed the probability that this particular vulnerability was exploited out of 100 you know 30 times. So, it is a 30, 0.3 probability you do not have that kind of data. So, we will just have to do this based on our own knowledge of exploits and what kind of attackers we have in mind.

who might be very very persistent attackers or whether they are just hobby attackers and so on. And based on that you will assign low, moderate and high and usually you would say low means about 0.

25 probability 0 to 0.25. 0.25 and 0.75 you might consider it moderate and then if you are above 0.75 you can say it is high.

But that number numbering could be points you know 0.3, 0.3 to 0.6 above 0.6 or you can also have more nuanced you know ranks for example you can have very low, moderately medium, medium, high very high you can have 6 different distinct points provided you are able to distinguish right. So, if you can, you might be able to distinguish in a very crude way that it is low, medium or high. You may not have the ability to distinguish it into 6 different buckets. If you can, then you can use that as well. You will get a little better estimates.

Defining Impact

- impact (Value)
  - Using the information documented during the risk identification process, assign weighted scores based on the value of each information asset, i.e.1-100, low-med-high, etc.

Sample Impact Definitions

	Confidentiality	Integrity	Availability
Low	Loss of confidentiality leads to a **limited effect** on the organization.	Loss of integrity leads to a **limited effect** on the organization.	Loss of availability leads to a **limited effect** on the organization.
Moderate	Loss of confidentiality leads to a **serious effect** on the organization.	Loss of integrity leads to a **serious effect** on the organization.	Loss of availability leads to a **serious effect** on the organization.
High	Loss of confidentiality leads to a **severe effect** on the organization.	Loss of integrity leads to a **severe effect** on the organization.	Loss of availability leads to a **severe effect** on the organization.

And the next thing you have to do is the estimation of the impact right. So, you can say how to go about estimating the impact right. So, one way to do that is if it is about data only right, is it about critical data protection right, then you can do it in this way.

It does not have to be this way because it is not always about data, it could be about disruption to your business process right. In that case this way will not work. You have to do it differently, but suppose you are thinking in terms of data. So, what are the three things that are crucial about data that I want to protect right? One thing is I want to protect the confidentiality and privacy of the data. I want to protect the integrity of the data, that is, I do not want some unauthorized person to come and change my data.

And then I also want availability, that is data should be accessible to legitimate users when and you know how they want to access it right. So, these are the three things right. So, suppose a particular threat if it is exploited if it is realized or exercised. Then let us say confidentiality will be lost, but the confidentiality of this particular data. The data that

will be lost is very you know it is not very important, it is not PII data, it is not personally identifiable information, it is just some data, some price list or something right. In that case I will say that confidentiality impact is low, now if that data gets changed maybe it will be it will have some limited impact also.

So in that case I will say integrity impact will be also low and then availability impact may also be low if it is not a DDoS attack or the server does not crash by this attack then I will say that the availability impact is also low. So, similarly you know it could be that the data is rather serious data and there will be a severe effect on the organization if that data gets lost or if it is people's grade then integrity is very important. So, in that case if integrity is lost that will have a severe impact. So, this way you can determine that in case of these threats, what am I going to lose is it data then what kind of data, what will happen if the data gets lost to the organization to the business processes that are bread and butter for the organization right. So, that is how you are going to do the impact and then with such a limited effect you can have a severe effect.

And you can also see it in terms of financial numbers right. So you can think in terms of mission capability by mission I mean business process like every organization has a business mission right to for example an organization must have a quarterly goal right. or an annual target. So, you have to think in those terms right. So, you have to say if there is a DDoS attack to our e-commerce site which was there for 2 days and which took us 2 days to recover, what would be the loss in terms of my, you know from my quarterly goal like how far I will be from my quarterly goal.

If you are not too far then the impact is not so severe. If it is very very far then let us say it is during the Christmas right. This is the highest ecommerce season and then you have a DDoS during that time. So, maybe the severity will be very high. So, you have to think in terms of those and then you have to see how bad is how bad is the impact on the mission of the organization's business mission. Otherwise you can also think in terms of financial loss. You can say it leads to this much loss or that much loss and then accordingly you can say high low severe etc.

Or you can think in terms of if it is a factory or something that gets attacked and there is a you know explosion or a conveyor belt in you know operational malfunction and all that stuff there could be harm to human lives and you can decide whether what will constitute limited and what will constitute severe loss. So, all these things have to be decided by who, right by the business itself right. So, when the risk assessor comes in, the risk assessor does not just work unilaterally; he has to actually work with the stakeholders inside the organization to define these things right. Because what is severe to you may not be severe to me like for example, 100,000 dollars cannot be absolutely right. For an

organization 100,000 may be nothing like you know Ambani's son is getting married right he is spending 120 crores right now 120 million dollars for a pre-wedding bash right.

So for him 100,000 will not count right. So you have to work with the organization to figure out what constitutes severe and what constitutes low and things like that right. So that is what you have to do. That is why you have to work with the organization as a risk assessor. You cannot do this unilaterally.

Risk Matrix

- **Sample Risk Determination Matrix**

		Impact		
		High	Moderate	Low
Likelihood	High	High	High	Moderate
	Moderate	High	Moderate	Low
	Low	Moderate	Low	Low

Now you have to work to create the risk matrix and this risk matrix also you have to work with the organization right. So for example if impact is high likelihood is high then most people will agree that the risk is high right. If the likelihood is moderate and impact is moderate most people will say ok the risk is moderate, but if likelihood is moderate and impact is low or if impact is moderate and likelihood is low whether we will call it low or moderate it depends on your goals.

Some Common Risk Assessment methodologies

- The following methodologies and tools were developed for managing risks in information systems:
  - National Institute of Standards & Technology (NIST) Methodology
  - OCTAVE®
  - FRAP
  - COBRA
  - Risk Watch

So you create this risk matrix and stick to it right. So you create this risk matrix, So if your likelihood is high and your impact is low then I will say the risk is moderate right.

That decision whether you will call it moderate or I will call it low is depending on you know organizational context. But once you have fixed it by discussing with the organizational stakeholders you stick to this you will apply the same matrix to all assets right you will not like to change it based on assets. So these are the risk assessment methodologies that are well known there is there are lot more nowadays, but these are some of the well known ones this is the NIST methodology is most commonly used, but there is Octave, FRAP, COBRA, RiskWatch there is also FAIR and few others. So, NIST is the National Institute of Standards and Technology that they actually do a lot of work on setting standards and frameworks and so on.

National Institute of Standards & Technology (NIST)

- **(NIST) Methodology**
- NIST Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems* is the US Federal Government's standard.
- This methodology is primarily designed to be qualitative and is based upon skilled security analysts working with system owners and technical experts to thoroughly identify, evaluate and manage risk in IT systems.

After this you know after we finish the risk, we will also talk about NIST Cybersecurity Framework or CSF. So, this is a, they publish, they do a lot of research and publish various methodologies, standards etc., and they have a naming convention for their documents. So, this RISK-SP special SP stands for special publication 800-30. So, this is about risk assessment.

NIST Risk Assessment Methodology

- The NIST methodology consists of 9 steps each has inputs and out puts:
- • Step 1: System Characterization
- • Step 2: Threat Identification
- • Step 3: Vulnerability Identification
- • Step 4: Control Analysis
- • Step 5: Likelihood Determination
- • Step 6: Impact Analysis
- • Step 7: Risk Determination
- • Step 8: Control Recommendations
- • Step 9: Results Documentation

This is used by the US federal government for risk assessment so what is there in the NIST framework? Different frameworks do it slightly differently and there are tools actually for this. Now one of the most common tools is Risk Lens, right. Risk Lens is a company that has a very nice tool for cyber security risk assessment of organization. You have to feed in lot of information into this tool, like you have to give it your whole you have to give it your entire network structure information, you have to give it application information, you have to give it business dependency information between assets and processes and you have to give do threat modeling and then you have to also give vulnerability information or the tool itself can actually go and scan for vulnerabilities in the various you know system if you if you wanted to do that and then it will actually help you do the risk assessment you know guided risk assessment, but we are only talking about methodology not tool. NIST methodology basically says that first you have to characterize the system that you are studying right. So, you have to go into an organization and you have to study the organizational system in order to do its risk assessment right.

So after that you have to do threat identification. So this part we have already understood that I have to first imagine what threats might be there to my organization and then I have to also do vulnerability identification. I have to know what vulnerabilities are there in my organization. then I have to see what controls are there. What is control? The control basically means any kind of countermeasures that I have put in, because I know I have done some high level risk assessment right. So, for example, So, you will not find any organization today, well maybe there are some, but very unlikely that does not have a firewall right.

So, most organizations will have firewalls. maybe they will also have antivirus on all their at least on their critical machines they might also have a few other things right. So those are controls right there may be other controls like for example they might have strong two-factor authentication requirements for all users they might have certain requirements for. what kind of passwords are allowed right. So these are what is what we call administrative controls. So there are technological controls like firewalls and antivirus and so on and there are procedural or administrative controls like making sure that the password rules are imposed or two factor authentication is imposed. These are administrative controls.

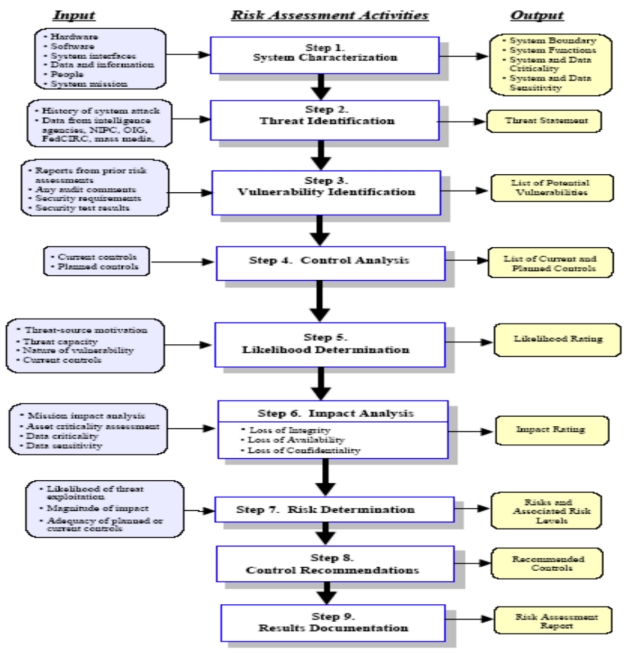
So every organization will have, as a risk analyst when you go in they already have certain controls. So, you have to see what controls are there. So, that is your step 4 to see what controls are already there and then whether they have any risk reduction right. So, the goal is to actually figure out what is the current risk right. And then you have to analyze which threat can be exercised or realized by exploiting which vulnerability that

will give you the likelihoods.

And then you have to do impact analysis. We have to figure out which asset you know will have a high impact and so on. And then from that use the risk matrix to do risk determination. And then once you have done the risk determination, you usually would determine the risk per asset. So, you see this asset is at high risk, that asset is at a low risk, that asset is at a medium risk. Now, I want everybody to be at low risk right, I do not want anybody to be at the high risk and operate with that situation.

So, I would then decide what controls will reduce the risk. What do I need to do, do I need to segment the network, do I need to add additional monitoring, do I have to do some you know deception techniques, do I have to do some kind of you know detection hardening etc. So all those things will come in control recommendation and then I have to document all this and that is my deliverable to you right. Now you know your risks and you have to. I have told you what controls will reduce your risk. Now usually after this once the organization gets the opportunity to put in the controls you recommended, they will call you again and ask for another risk assessment to see what is the residual risk.

The risk that remains after all the controls are put in is called the residual risk. So, you have to also figure out whether the residual risk is acceptable or not and what kind of risk is acceptable is a matter of business decision that has to be taken also by the client organization not by the risk assessor. Risk assessor will tell you what the risk is and then you have to decide whether you want to take more than that risk or you want the risk assessor to suggest additional control so that your risk is even further reduced, but you get the basic idea right. So, now you can go and go to a company and do risk assessment if you have a job right.



Now it is not always that easy. So, this one is from the NIST document. Basically it says what kind of information you take as input. for every step and what is the output right. So, every step is basically an activity right. So, for every step of the activities you have to give some information like, for example, system characterization. This is the most time consuming part of risk assessment because most companies do not have a proper inventory of their hardware, software, applications, their versions, what software they have, what version is there, which one has which patch version and so on.

Then you have to also know the system interfaces, that is how they interact with the outside and how they are connected to each other. You also have to know the data and information that is there inside the organization, whether there is personally identifiable information, whether there is any other business critical information, intellectual property, etc critical information and then you also have to know what the people are. So, a cyber security audit is about compliance rights. So, compliance basically says that let us say let us say your regulator wants you to be 27 ISO 27001 compliant. So, an auditor will come in and check everything against the requirements of 27001.

And you know irrespective of what the risks are or anything right. So, you will say ok 27001 says that you have to have this kind of controls and whether you have that or not they will check or say that you do not confirm. So, audits are about compliance. So risk assessment is for knowing yourself and what you need to do right. So nowadays actually if you read the 27001 standard or 62443 standard they actually say that you start with risk assessment and then you put your controls, do not blindly put controls then when the auditor comes the auditor will check whether you did the risk assessment.

right or are you putting controls arbitrarily as you please. So risk assessment will be at a checkpoint in this thing. How many times risk assessment is done you know poorly also right. So because as far as audit is concerned whether you have done risk assessment whether you have a risk register. So, at the end of the risk assessment there will be a risk register which will say which of your assets has what level of risk and what you have whether you have done something about it or not. So, the auditor will check whether you have a risk register or not.

So, you can make an arbitrary risk register and show the auditor that I have done my job right. So, it is all about. This is a big struggle that you know people are having nowadays and we had this people from MITRE also last week and so you see governments are very concerned because people are not taking cyber security as seriously as they should right. And especially if you think in terms of power generation companies, power transmission companies or oil and gas companies right. And the problem is that they are always thinking that it's ok.

So, the government requires me to have 27001 compliance. So, let me somehow get the compliance checklist done right. They are not thinking of it as something that is good for themselves. They think it is an obligation that they have to decide whether they know whether their system is secure or not because they are. board level people are not understanding the importance of cyber security or the lower level the chief risk officer or chief information security officer is not telling the board what can go wrong in case there is an attack and what kind of business losses might be there, what kind of regulatory penalty there may be there and so on. So, therefore, there is a tendency to do these things in a short time with a shortcut and so on.

Interestingly another problem that we face as C3iHub as a company is that when we go for so we do VAPT and audit for organizations. Now obviously we try to do it in the most elaborate way right. Now when you try to do this in the most elaborate way, there are two issues. One is it takes time and then it also takes money. So you have to send your engineers several times to the organization. Now when you go for a tender, there will be two people, and a five person company will bid for it for a very small amount, like 50,000 rupees.

and we cannot do below 5 lakhs for example. I am just giving an example, not that number. So obviously now the company that is serious about cyber security will probably say okay fine I am going to pay more because I want to actually check my cyber security situation. But a company that is doing it for compliance as long as the company there is a cheaper company willing to give them a compliance certificate. they will be happier right, so this is a big problem. But in any case coming back to this, basically for system

characterization you need to have all this information about the organizational assets, hardware assets, software assets, remember people are also assets and so on. And then you get the output of system characterization, you get system functionalities, you get system boundary, you get the characterization of the data and all kinds of sensitivity of the data, which data is critical, which data is not.

So, oftentimes we find when we go for doing this system characterization we find that they do not have a network diagram right. So, there was a big ransomware attack on one of the biggest hospitals in India. So, our guys went the next day and then they asked for the network diagram. And, these guys had a hand drawn network diagram in some place which is very old right.

And, then they found that that network diagram is very pretty old. So, it is not reflecting the real system that is in place. and then they found that there was a bypass. They bypassed the firewall to a major server right. So there is no firewall to access a major server. So at the end of this system characterization you get a clean network diagram so many times our engineers actually go under the desk to figure out the trace of the connection between two servers like you know how they are connected to each other to create the network diagram. So, at the end of this system characterization you will get this full character like if you do your job well you will get a full network diagram you will get the list of all hardware software there what kind of patches they have and all that stuff.

So threat identification has many different ways of doing threat identification. One is you have to know the history of attacks not only to your organization but to other similar organizations right. You need to understand what kind of attacks can happen right. You can also get data from various threat intelligence companies from mass media and also from regulators and so on. So you basically have to this is a place where imagination can help you a lot right. What kind of attacks can happen? You have to think in terms of like an attacker, like what are the different ways an user may want what an user may want from me.

So any of you have watched this TV series called Mr. Robot. So if you watch Mr. Robot then you get some good threat intelligence ideas right. So this guy is and all the attacks that they show in Mr. Robot are actually brainstormed by real hackers. So all of them are realizable.

So for example you want to so there is data. that has been wiped from financial institutions. They have backup tapes in one storage right. So the hacker actually attacks the air condition system of that building to raise the temperature so that those tapes get

destroyed. So, you have to be imaginative to think in terms of knowing what threats can come. So, then you can actually get this you know what threats can happen. So, you get a threat list. And then you have to do the vulnerability identification right so here as input you have you know various things, reports from prior vulnerability assessment, any kind of audit observation and various security requirements and then you get a list of potential vulnerabilities right.

Now you have the control analysis, so for control analysis you have to know what are the current controls and what are the controls that are currently being planned, because if something is being planned you can you may also consider that, depending on how far out the plan is, if the plan is 3 years from now we will have a firewall that is not a serious plan but if it is like we are the firewall is in on order we are going to get it and going to segment the network maybe you can consider that. But in any case you look at these controls and you basically say ok these are the list of controls that I have to consider when I am going to do the likelihood computation, likelihood determination. So you then get these threats, you look at the threats and then you have to also see what the threat sources are right. So some threat sources might be hobby hackers, you do not take them that seriously as if the threat source is advanced persistent threat group or a nation state attacker right.

So, you have to consider those. And then you have to see what is the capacity of that threat group and then you have to see the vulnerabilities that can actually exercise that threat. And then you have to see whether the current controls will reduce that possibility and reduce that likelihood. Having considered all those you will say I have a likelihood rating for every threat vulnerability pair.

So, I have a likelihood rating now. Now I have to do impact analysis. So, for impact analysis you have to see what my business process goals are, you have to look at asset criticality, you have to look at data criticality, data sensitivity and so on. And then you have to see how you want to do the impact analysis and you get this rating of the impacts. and then you use the risk matrix to compute the risk for the various assets and now you do a control recommendation that if you put this controls then you will reduce the risk and then you do the documentation and then you do your first phase of risk assessment. Usually then you have you give them some time to put those controls the ones that you recommended then you go back and do another risk assessment to see whether the residual risk is acceptable or not.