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: 03
Lecture: 09

So, good morning everyone. Today we will be presenting a case, the iPremier company case. It is on distributed denial of service attack. So first, we will start with a small introduction to the company. So iPremier company is in the e-commerce business and their product which they sell are luxury, rare and vintage goods. So the prices of the products range from hundreds to tens of thousands of dollars.

Their clientele is basically a high-end clientele. So their customer trust with the products which the company is selling as well as the services offered by the company is going to be very crucial for the success of this company. And in 2017, they have over 1 million regular customers in their database. Regarding the competition that the company faces, iPremier is already one of the top two websites in that field.

Their main competitor is Market Top and though the product is the main good which they are selling here, they feel that the competitive edge which iPremier enjoys is actually the user experience enjoyed by the customer. So basically on attractive websites, the after-sales service, the seamless service for the customer while purchasing and using the goods. Coming into the management culture of the company, so the company basically comprises of younger long-term employees who have been there with the company for long and experienced lateral hires. So the salaries are above average salaries and mostly the above average part comes as stock options for the employees and the compensation is linked to the performance. So the entire atmosphere is very very intense and with quarterly reviews and removal of unsuccessful managers.

So basically the characters in this case study are Bob Turley who is the Chief Information Officer and he has just recently joined the company. Next we have the CEO, Jack Samuelson. Bob Turley feels that he enjoys the confidence of the CEO, even though he has just joined really recently, because right now, he is in New York with a high profile assignment. Tim Mandel is the CTO, Chief Technical Officer and one of the co-founders of the company. Bob Turley has a good working relationship with Tim Mandel.

Next character is Warren Spangler who is the Vice President of Business Development and then we have Peter Stewart who is the legal counsel for the company and who is providing the legal perspective to the various incidents in this case. Joanne Ripley is the

Operations Team Leader who is taking care of the cyber security operations for this company and Leon Ledbetter is another employee in the Operations Team. We have developed a storyboard kind of presentation, explaining what is happening in the case and we hope you enjoy it. So the events in this case begin at early 4.30 am in the morning.

So Bob Turley gets a call from Leon Ledbetter from the Operations Team. So, " Why are you calling me at 4.30 in the morning, Leon?" " Mr. Turley, we are facing trouble accessing our website and we have just been receiving mails which says - Ha Ha Ha. I am new to the organisation and have no idea what I am supposed to do.

" At this moment Bob Turley decides to directly call Joanne Ripley who is the Team Leader for the operations. " Okay hi Joanne, can you say what is going on actually?" " Bob, right now I am not sure what is happening but it actually does not look like a simple DDoS attack." So while this conversation was going on, Bob Turley is interrupted by another phone call. This time it is from Warren Spangler, the Vice President of Business Development. " Hi Bob, I hear something is happening and I am sure stock is going to take a hit tomorrow but you just don't have to worry about it" I will handle the PR.

" " Okay thanks Warren and we are also working from our side to achieve the best solution that is possible. Thanks for your input." After that interruption Bob Turley goes back with his conversation with Joanne Ripley. " So Joanne, can you tell me now, do you have any emergency procedure since the attack has happened or do you have any incident response team or crisis management procedure which we can follow now?" " Bob, actually we have got a BCP but it's not been updated and we actually haven't practiced incident response." Bob Turley had actually expected a company like iPremier to have an updated disaster response plan and an incident response plan but he was surprised that they didn't have all that but he also realized that it was his responsibility as a CIO to have looked into these issues.

So now he has gone back discussing other options with Joanne Ripley. " So Joanne, so what is next? What are your options and are they stealing our data?" " I can't give you an answer right now. I am not sure what's happening. Let me first go to Qdata where our server is and access the web server to see what's going on." So Qdata is the data server for the website and they have been a long time service provider for iPremier.

However iPremier knows that they are not actually a very competent service and the only reason they chose Qdata is because the proximity to the office. Now Bob Turley decides he needs to call Tim Mandel, the CTO with whom he has a working relationship and to get some advice on how to proceed. " Hi Tim, hope it's a very exciting morning. So it seems like we are being under attack and so should we proceed by cutting the connections?" " Cutting the connection, I would not recommend it but we might because we might need some evidence but it is highly unlikely that we can preserve the log data." The log data detailing feature had been removed as a part of a measure to increase the customer experience by 20% because that will delay the interactions.

So that feature has been removed and now perhaps they might be rethinking about that." This time, another interruption and this time it is Peter Stewart, the legal counsel. " Hey Bob, it is Peter Stewart from the legal counsel. I would recommend you to completely cut the connection because it will risk our customer's personal information." " Okay, I understand your perspective, Peter.

So thanks for the input and I will see what I can do." And now Bob returns back to his call to Joanne. So, " Hi Joanne, what is in, any update?" " Bob, they are not letting me into the building. Can you please escalate this issue? It's very urgent you know what it is. Now I think, it is an attack on our firewall.

" So this time, at 5.27 Jack gets the call which he had been hoping he would not get. This is from the CEO. Bob gets a call from the CEO. " Bob, this talk is probably going to be impacted and we will have to put a solid PR phase on this but that is not your concern right now.

You should focus on getting us back and running. Understand Bob?" "Yeah, sure Jack and though everything is not going according to our plan but still we are working our plan and we will try to get the best solution. Thanks for having my back." " So hi Joanne what's the situation now?" " Bob as expected, it is a DDoS attack. It looks like a SYN flood from multiple sites has been directed on the router that runs our firewall.

" " So what can we do right now? Is the customer data safe at least? Are we sure of it?" " I can not cut the traffic in as they are spawning the zombies. There is nothing that makes a DDoS attack and intrusion mutually exclusive. So I am not sure if they are stealing away our customer data." Okay, at 5.26 the entire attack suddenly stopped and Joanne now calls Bob again to give an update on this new development.

"Hey Bob, the attack just stopped. It just stopped. I did not do anything. " Oh my god really? So I mean, what are we supposed to do now? To just cut the connections or can we resume the business as usual?" " The website is perfectly running. We can resume the business as usual but I recommend we shut down and let us search what the issue is.

" " Okay I will consider." So at the end of all these events, Bob now has to make a decision and he knows that his advice is the one which the company is going to follow. So basically he has four perspectives from four different people starting with the CEO who wants to get the business back up and running. At the same time he wants to ensure that the customer data is protected and there are no legal backlashes to whatever action the company is going to take. At the same time he is looking at his Ops team leader, Joanne Ripley, who has recommended that they shut down everything and get expert cyber security consultants to go over the entire system and check if there are any time, ticking time bombs or any customer data breaches which they have not actually known about right now. On the other hand we have the senior management from the business development side who is represented by Warren Spangler who has already mentioned that he wanted to, he has a personal motive in this because he wanted to encash his stock options so he wants to get the business back up and running because the stock prices will take a hit for a long time.

And finally we have the legal advice, legal perspective provided by Peter Stewart who has called for, had asked to cut the connection and to protect the personal information and avoid any legal consequences. Based on these four inputs and perspectives, the decision will have to be taken by Bob Turley Okay, so now coming back to the case and the presentation. So we've been hearing DDoS attack, DDoS attack in the whole presentation, that is what the iPremier had faced. So let's just deep dive into what DDoS actually is. So DDoS stands for distributed denial of service and is often used as a network attack and these attacks are a subset of denial of service attack.

So what are denial of service attacks? So these are attacks where the attacker attempts to, you know, overwhelm an internet connected asset with the aim of making it unavailable to the legitimate user. So an analogy for this can be like, if you have been someone who has been travelling in the public transport, always every time, especially in the Mumbai local, if you have travelled, the doors will be always crowded with passengers. So the legitimate user who needs to step out in the station, might not be actually able to do that. So this is what actually denial of service attack actually does to victim's, you know, server. Now that we understand what denial of service attack is, let us understand how is DDoS different from DoS attacks.

So in DoS attacks, it just uses a single source device and then creates fake traffic and exhausts the server resources. And this usually occurs in a very smaller scale. And in attacker's point of view, it is actually very easy to identify the attacker in this case. But then DDoS is a higher level of DoS attacks. And as you, it uses multiple systems to send real time traffic in order to overwhelm the victim's server.

So let's just have a quick look on how DDoS work. So the attacker actually infects a set of devices using a malware. This malware can be sent using any uniphishing mails or messages. And once the attacker attacks all the devices, these are in control of the attacker. So these systems are commonly in cyber world is known as botnets and the network connecting all of this network consisting all of this botnets is commonly referred to as the zombie network.

So the zombie network is the network that the attacker controls to flood a targeted website or server with traffic. And this is how the attacker is able to crash or disconnect the victim's server from the internet by flooding a lot of traffic into the system. Now let's talk about the DDoS attackers motivates. So a motivation, so it can be either hack activism. So in hack activism, it is a form of activism, which we normally see in our scenario.

But in this case, say for example, this is our e-commerce giant. So there is somebody who has a bad feeling about the site, just wants to shut down the site in form of an activism can do this. It can be cyber vandalism, it can be a cyber warfare. It can also be an extortion in order to get money from the company or it can also be rivalries as we have already seen, this is a highly competitive e-commerce platform and it has also have high competition. So in this case, we are not sure what was the motive but these are some of the motives, we have identified.

Next, coming to the analysis, what do you all think that actually went wrong? You can answer this based on today's, in the light of today's class, that we had. So you can answer it based on the managerial perspective or the technical perspective. Actually, based on the case study, iPremium, they were lucky and fortunate that it was just a failed attack or attempt. The website was not actually hacked but they were actually in the business of, you know, catering to all the premium customers and all the credit card information and all. So I think based on the options, that four options you were mentioning, they should shut down their services and do some introspection and they should really invest to upgrade these cyber security measures and all.

This is not like a failed attack. They did attack. It is a DDoS attack. But yeah, we will be considering the options in the later. The hacker was actually not that successful to hack the website.

So that damage was not there. We are actually not sure of what exactly happened. We will be dealing with it right further. So right now in case, given the incident What actually went wrong? Like the managerial side. So I will talk about the technical side. So they had given the entire technical management to QData, which was actually not investing in advanced technologies.

That was one of the main reasons. And also one of the founders of this iPremier company, had a personal relation with QData. So it was not also ready to go for other companies. That is an answer. Another one aspect which is highlighted in the case studies is that they had an emergency response plan, but it was not updated with respect to time and most of the contacts and all were not updated. So that is one aspect which they need to update all the emergency plans from time to time.

From a management perspective, firstly, it is described that there was a very intense working culture and variable pay of the specially senior managers, managers was entirely based on stock options. So the senior management's focus was on driving the stock price up. And that led to various steps like they should be very intense, trying to get sales, trying to have the website up and running all the time without so much focusing on consolidating what they had already achieved as their customer base, looking at the risk part of especially cyber security. So there was never, I mean, like he mentioned, the business continuity plan was outdated because there was never a focus on it.

There was no disaster recovery plan. There was no incident response plan. So there were a series of effects from a management side because of the entire focus on driving the stock price up. With technical perspective, they were not storing the log data. They made a compromise in storing the log data. which will lead them to not able to investigate the case in the future and identify what was the cause and found out who did it.

So thank you all for the response. You were all correct. And in light of today's class, if we are to tell a verdict, the thing is that the company, iPremier did not consider cyber security as one of their strategies. They didn't give priority and has been rightly pointed out by Sir. It was the stocks or it was the profits that keep them driving.

So they lack security and risk expert. And as we studied in today's class, actually being an e-commerce company, a top e-commerce company, they should actually follow some sort of a framework or at least take into consideration the ISO standards or any other standards. But they failed to do that and they did not also have a contingency plan as well. So now as Sir already told in the class, thanks that this attack actually happened. Now that iPremier will be more into the cyber security and might take this as a strategy. Now handing over to Nithish, to check what all can they do forward.

So now again back to you guys. Let's now consider for a moment that you are Bob and we will let us continue with the case because now the case ended at Joanne calling Bob and saying that the attack has stopped. And now Bob is in the position of making a decision because Joanne said that the attack has stopped and the websites are up. So they can either continue to resume their business as usual or they can shut down the systems, I mean the servers and then collect the data to identify what type of attack was it, from where it originated to understand more about the nature of the attack. So considering that you are Bob, can you guys throw a light or what should be best, should be done? Should they shut down the systems or should they be resuming the business as usual? Any idea? Yeah, over to you. I feel that they should shut down the system because rather than going by the personal interests of the people in the company, they should not be exposed to any other attack by any hackers here after.

So it's better to shut down the company, I mean shut down the system. Okay, good. So first of all, it was the even we are suggesting the same thing. Our immediate course of action should be to shut down the server systems to collect whatever data is actually present and you know even in the short term long term to conduct a thorough forensic audit. And the major reasons as already mentioned would be to understand more about the nature of the attack and as Sir, as rightly mentioned in the previous class, hackers try to exploit the vulnerabilities present in our system.

So we should be able to be in the correct position to identify the vulnerabilities present in the system. This will also help us to safeguard from the future attacks. And now what will be the second immediate course of action? So considering or take it up more as a follow up question. So consider that you are now shutting down the servers. What should you be saying to the PR? Should you be saying that it is a regular server maintenance issue which we are trying to solve or do you want to disclose that a cyber attack actually happened and we are in the process of rectifying it? So what would be your opinion on that? Yeah, I think that they should disclose that it was a cyber attack.

Because if there is any ethical problem in the future as a good governance and ethical structure that a company has to follow, I think that they should disclose because that would improve their trust among the stakeholders that they have actually disclosed the vulnerability that they had. So I think in the future perspective, it is better to disclose. Yeah, so you are right. Because first they should dealing with the PR team and maybe they can issue a press statement or at least a tweet which has been done recently saying that there was a temporary, unusual, irregular attack that has happened on our systems and they can say that they are trying to give more importance to the customer's privacy and hence they are trying to resolve the issue ASAP. And the main reason for this is that first of all from the company's perspective, they are responsible for what had happened because they did not have a proper crisis management team or even an incident response team.

So first of all, they are responsible and it is better to disclose it. And moreover from the legal perspective, tomorrow if any customer comes up saying that my data has been stolen and even if they try to sue the company in such cases if the company has already hid the fact then, it will be a major damage for the company. So considering the future actions as well, it is better to disclose and that is what even major corporations like LinkedIn, Gmail, they do. Whenever they face an attack, they openly try to admit what has happened.

So this would be the immediate course of action. And well, now let us also consider long term alternatives. Considering this happened, we have also tried to come up with long term suggestions which the company can follow and we have also listed them in the descending order of preference, our team's discussions preference. So, the first one would be to replace Qdata that is, to outsource or contract a new service rating company for proper security reasons because we already saw that Qdata security management was outdated and they also had a problem in retaining the staff. And the second alternative would be to develop an internal IT system, that is insourcing their own cyber security management and setting up their own teams and the servers and get them back up running. And the third alternative would be to recreate the whole architecture which is by staying with Qdata but updating their own mechanisms whatever they have, so that their long term commitment also still continues while updating their procedures.

And to be a bit more elaborative, we have also come up with the pros and cons of each alternative so that it will give us a better understanding, while in the descending order of preference as already mentioned and I will quickly go through these. So the main pro of replacing Qdata is that they will be dealing with, they will be outsourcing to a major, either the top market player or major market player so that they will be obviously having the state of the art infrastructure and they will be having improved defence mechanism with constant updates and patches, which unlike how Qdata was obsolete. And they obviously, post the attack if they are switching to a major player it will also have a positive attraction over the public and leading to increased customer trust. And the three major disadvantages would be that now if they are switching they have to work from the scratch because obviously and this will also lead to increased spend on financial resources. And it will also be time consuming process because they have to migrate the data from the old server to the new company's servers and there will obviously be a lot of switching cost as well as time consuming process and moreover third point as mentioned, it affects the personal commitment with the owner of the Qdata but again at the end of the day, we have to do what serves the company best and that is why we have we are, we consider this to be the best alternative.

The second would be to develop the internal IT system because as mentioned in the article, it has already been mentioned that insourcing their own cyber security management team has been in their cards or in their bucket list for a long time but they have been prioritizing their sales as what one of our fellow mate mentioned because of the stock options and other incentives. So a good time would be now to refocus their priorities and the main advantage of this would be that, they will be having full control over the database system as well as cyber security team and since that has been insourced they will be quickly able resolve the issues, whenever they detect. So and moreover it will also be cost effective in the long run but not in the short term, but definitely it will be cost effective and might even save a lot of, you know, billions of dollars of revenue for them in the long run and again the major disadvantage would be, it will be costly however they have to install the servers they have to hire a new team, maybe a lot of team cyber security teams you know crisis management teams and everything obviously it will again be time consuming and outcome is not guaranteed because you know, when new types of attacks start coming up daily cropping up daily, so they will have to be constantly updating, so they might not be as effective as the new market player but still this can be considered worthwhile. And now, the third alternative would be to retain their relationship with Qdata while recreating the architecture but again the advantage would be that it helps avert the switching cost to a new market player for iPremier, it helps them save time in returning to normalcy, compared to switching and migrating their data and moreover the long term relationship is restored but the con is that if we never know because already Qdata is performing bad and we never know how ready they are to accept to modify their terms as well as to their technology and this updating process might again take a significant amount of time that is why we consider it to be the last option in our data.

So we consider this was and hope insightful and enriching session. If you have any questions, you can follow. Excellent presentation but I disagree with you. So your suggestion is that the company shuts down and does forensics, examines intensely whether customer data has been stolen and put in place cyber security systems and then restart their business and what is the guarantee that when you do all this and restart your business, customers will come to you because it is a very competitive market. There is Market Top which is the major competitor and this is niche product or high end products that they sell online and it is online, the moment the customer feels that my data is not secure and it is not secure to do business with iPremier I may not come back, you shut down, you did a lot of things, that is fine. I have competitors to go to, so you may be actually shutting down your business itself you may be closing your business, if you shut down and go for IT maintenance for a long time.

So what do you think about it? Sir, if you are not following this procedure as well, we believe that the company might shut down because again, we are not sure what has, who caused the attack and what has been stolen. So if we try to resume the business as usual it might go okay, fine, for a shorter period of time but we should also remember that the person who are targeted also had the audacity to send a Ha Ha email messages. So it means that it was a proper targeted attack and it is, we can be 75 percentage sure that there was some data that has been stolen or they might have even installed some bots that might be transferring data internally, without us noticing it. So considering these security risks, if we try to resume it as usual business might go but later on people, this hack, some other external party Business is gone.

No, if you're hiding the fact, if you're hiding the fact. See the issues of customer trust so if you hide that information that this attack has happened, then this information gets revealed later by whoever has done the attack, it might be the competitor himself is doing this attack on us and he reveals it, then the loss of customer trust later when customers find out that, high level clientele find out this company has been hiding information from me, it will be greater than what will happen now, right now we can take ownership of the situation and try to reassure our customers that we are working on it, there will be loss of customers. So this is about shutting down your business or closing your business versus what potentially can happen in future which, if there is a way to manage that, you may still be able to run your business. The other aspect which you are not considering is about job security. So this is Bob and Bob is in the stock market I think he is in New York, taking care of company's stocks or publicity but the company is attacked and at the bottom, right and it may not exist tomorrow, so won't some people be trying to safeguard their jobs because this is a company which easily fires people and you know somebody has to take ownership, you know that they are also trying to pass bucks or you can see they are trying to safeguard their jobs also. If you read it carefully, so if Bob does not have job tomorrow, how would the behaviour change? Well, actually the point is during the case itself Bob develops a new reason , he says, " I have been there only for three months, how will you expect me to handle such a big crisis ?" So he has already developed that excuse which he is going to say, however the CEO calls him he gives him a very professional answer, like you take care of this problem you get the business back up and running, which is your job.

and he doesn't tell, he doesn't do any reprimand of Bob or no blaming of anybody he wants that in process business to continue, so since the CEO is so focused and more professional in that manner, we can Bob can hope that he might still have his job and at the same time what Bob says is correct, he is only been there for three months and perhaps he has been he has overlooked the fact that this company, new company does not get updated its business continuity plan binder as well as the incident response plan. So those things are things which he is going to be working on after this and Joanne Ripley, in the final part of the case also mentions when she accesses the data center, she talks about the firewall and she just makes the statement that the firewall is so bad, we should actually work on this, so she has been there for a long time. So with regards to job securities since the company has not focused on it or made cybersecurity a strategic priority which is a high level decision which the CEO is also going to be involved in making such a decision

So job security is not going to be much of a issue right now and moreover the blame is partially on each of the senior managers right from not having an updated binder, so everything from having not checking the proper firewall, not checking the contracts and Qdata and everything, so partially everyone is responsible, so we have to come to that and make a decision yeah, yeah, so we are discussing what is internal now, but essentially your decision will have an implication for survival of the company and on the market so if you are going by shutting down, then what is your PR strategy? Because what do you communicate to people, we are shut down because we are under cyber attack may not work, the PR strategy is, as Nithish had mentioned, would be like we would send an immediate tweet or notice that such an incident as high level and high level of traffic has been observed in our data which is not as part of the usual behavior and therefore we are shutting down this website to do some routine maintenance and check for any vulnerabilities We saw that most of the big players like Google or YouTube, they have also faced similar situations and Amazon whatever so everybody has faced similar situation and what they actually did is, they have told the public this is what is going on, so it is always better to let the public know exactly what happened and I also suggest that not let the public know exactly what happened but we can say that we are suspicious of some irregularities, irregular traffic in the system, so we can maybe play with the words because when we did some secondary research on what the major corporations did, actually the proper forensic data audit takes months or even years to come up with a proper report so maybe initially what happens is the major corporations release a statement saying something has happened then they are trying to get it back and even after some few business days, four to five, the business comes back usual and starts running but the final report of what exactly happened there is some corporations released years after. For example, in the case of LinkedIn it was after three years, they later came up and said that these many number of accounts have been lost or they are in the jeopardy of losing their information. So the aftereffect might be even be a bit later, but right now, shutting down for a few business days is a better option is what we consider and we can let that know to the PR team as well.

So choosing among the which is the lesser evil that is what you are actually but I think the most important thing to consider is the fact that this is a company which is in high competition, it is online and it has to continue its business, any option that leads to bankruptcy or closing of business, although it may be technically correct but it is not correct for business, so that is the tension that we have here. So there is, these are all risky options but you have to choose among them. So therefore that is why he asked what is the PR strategy ? If you are going by this then there is a public statement one has to make why the business is shared and that is a very very important statement and in one of the cases that come up, that itself was a discussion and you can see how they made a public statement, maybe the PR becomes the most critical aspect of your decision. On the other hand you already evaluated if you go by, well business as usual it is much more risky I would say If you know the reason, as to why the attack happened, you know there was a failure and while the failure happened is very clear to the organization or to the technical people, then you are fine you have actually addressed it, now you can go forward confidently if you have taken corrective action and preventive action, then you can go forward but in this case the attack just stopped, the attacker stopped .

They were at the mercy of the attackers. They just stopped. So somebody is having fun and you have not really diagnosed what was the problem, so you can do what prevents the attacker from doing it again and therefore there is no option but they have to actually find out, so that can further strengthen as to why the attack stopped they do not know. If they run the business again another day, it can happen in the same way so therefore it is important that they stop there and diagnose correct and then move forward okay, so that can be a strong recommendation, okay so let us wait for the B and C. Is there any other comment ? Regarding the recommendation right, the second point what you have said regarding the exposure to the public with the PR announcement, during the incident the management also concerned about the stock market which may affect their business and if you see about the instance timing it was a DDoS attack which has happened in the early morning around 4 or 5 which is a non business service in perspective of a business but it is since the e-commerce most of the customers would not be able to use that same and moreover maybe 90 - 95 percent of the customers do not even know that the attack is even happened or not, so is it correct for the PR team to make an announcement which may affect their mark market or stock market when most of the customer did not know about this attack ? So whether it is good for the PR team to make it such an announcement. Say , for example in future they come to know, the public, that this attack has already happened and the PR is just issuing a statement without mentioning the attack but it is server maintenance and in the future if someone from the public says that, okay, my personal data has been stolen, then again this PR only will have to face the public.

So it is always better to reach out to the public and say what is happening. That yeah, my concern is you know shut down for how much time? what do you visualize how long it is going to take to implement all those safety measures and upgradation of the system, normally normally how much it takes ? Yeah, so it depends on the scale of data and normally when we did our research like in two weeks or sometimes even business days might take the data how much is the attack? So in our case, we really do not know the scale of the attack but like when we did our secondary research what we came to know that it depends maybe just days, one or two days or it might also extend till weeks Yeah, this is the CEO's question, that is the CEO's question, you want to shut down for how long? So that is the first question anyone would ask and you don't know actually sometimes, right and that answer is not acceptable, you know this is the sort of real-life scenario that you will come across, they want you to tell the time but you do not know, you know so uncertainty is not acceptable. So but you are thrown into a situation like that, you know at this moment and that is a dilemma in the case and you know the other thing that one of the participants suggested that, that is that is normative, they should have had a parallel system You know, so they should have a hot site or a warm site or a cold site, some thing to switch to, when an incident of this happens but actually it is not there, they did not have, they did not have any strategy cyber security strategy they had to build all those, so you can just be wishful this should have been there ,that should have been there, in this case and should be should not take much time, you know tell me how much time, nobody is in a position to say anything and that is a sort of attack that is depicted in the case. That is the sentence you know so it is an eye-opener for the organization this organization can die or can go forward, we do not know so the case actually presents a real-life situation where if you are not prepared and you are online, you can go out of business, if you do not have cyber security measures so we will wait for cases B and C with the sequels of this cases to understand more about what happens next, okay, in the next class. All right, thank you very much.