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: 04
Lecture: 12

Good afternoon everyone and welcome to the part 2 of the case which is iPremier Company's part 2, distributed denial of service attack part B and C. The group members are Lokesh, Sanjana and myself Subisha. So, let us go through a quick recap of part A, which the previous team had already discussed and these are the main people involved and Bob Turley who had recently joined as the CIO is faced with a very grievous challenge that is a DDOS attack for which they had not been prepared enough. So, these are the people, Jack Samuelson is the CEO and he had already warned Bob Turley about the operating procedures deficit which is there in the company which he had to tackle, but this was in the back of Bob Turley's head and there is Joanne Ripley, who is the operations team head who is running behind the hosting data company and the iPremier and there is the CTO Tim Mandel, there is a legal counsel Peter Stewart and Warren Spangler who is the VP of business development who is right now very much thinking about the stock prices rather than the security measures. So, the story till now is that iPremier is one of the top two retail chains that are existing right now and most of these customers used credit card information that is why they are very much worried about whether the customer data has been leaked or not. So, this company had an intense work culture in which only talented people only the younger people were retained mostly and the technical architecture, they were not giving that much importance and they had given it to a hosting company, a third party Qdata, which had outdated architecture and the staff attrition rate was very high in Qdata as well.

So, the attack which was a DDoS attack and this complicated the system because there was no detailed logging as such which was there in the iPremier company and they had not invested in good firewalls to defend such a attack of bigger scale and there was as we have seen all these contingency measures like BCP, IRP, DRP, nothing was implemented and in place. So, so the end of the attack was automatic and basically iPremier had no role on it and they were unsure in part A whether the firewall was breached or not and they were also unsure whether the customer data was leaked or not. So, there there are only two options either to shut down and rebuild completely or disconnect temporarily from the internet or continue as usual. So, basically these are the reasons that went wrong, that is why iPremier has come to this situation, the technical issue is that there has not been any detailed logs till now.

So, the recovery part is very difficult as of now and there are many DDoS protection softwares that are existing in the market, but none of them have been used by iPremier or Qdata. So, the firewall was outdated and was not able to handle this amount of traffic and the service also lacked the capacity to handle this much traffic and also they were thinking of moving to an internal IT team which has not formalized yet and the managerial problems are that, it was much of a young workforce, who had lesser experience and the Qdata should have been replaced a long ago, but it was standing still due to personal interest and a greater investment was required in security which was not invested and as I already said there are no emergency firefighting plans and there was no simulation attack or routine checks of security infrastructure which were in place and even they had not even thought about a PR strategy to tackle such similar attacks. So, and also Bob had not taken the advice of Jack seriously which was about the deficit in operating procedures. Now, we will move on to part B and C to know what has happened. Okay.

So, I will be discussing part B of the case. So, previously as she recapped the company is not sure whether they should disclose publicly about the attack. So, what iPremier actually does is a few hours after the attack they actually disclose publicly that they have been a victim of the DDOS attack and the attack lasted for a period of 75 minutes around midnight and post this they actually implemented new security measures and this is actually more reactive rather than proactive as we saw in today's class. So, I will be discussing about the security measures in the following slides and one important thing to be noted here is that they were not sure if the firewall is breached or not. So, they tried to gather evidence whether the firewall was breached or not.

So, how did they do that? So, they examined files on every production computer and it was examined on the basis of the identity and the size, that is probably the name of the file that is to check the identity and the size of the file but they did not check whether the contents of the file were altered or replaced and they did not have a mechanism to check that. So, now Ripley who is the operations team lead had to make a decision in such an uncertain situation and he recommended that all the production computers had to be shut down and they should be disconnected from the internet and they had to rebuild the software system using the developmental files. So, these development files were less likely to be tampered. So, they were used to rebuild. So, let us see what they actually do.

So, first the security measures instituted were, they restarted all the production computer equipments. So, these were done in a phased manner because if all were done at the same time, it would cause inconvenience to the customers. Next they conducted a file to file examination. So, this was done to ensure whether all the files were actually existing in the computer, I mean, in the system or not. Then they had a study on the technology solutions.

This was done to see whether the files, all the files were present and whether the content was altered or not. They also had a project to move to a more modern hosting facility. They modernized the computing infrastructure to build a more sophisticated firewall. They brought additional disk space and enabled high levels of logging. So, as she mentioned earlier they had actually disabled detail logging and this was done because this would cause a performance penalty of 20 percent.

So, the company actually wanted to focus on performance and they did not pay much attention to the security measures which was again a mistake that the company did. And last the next they also trained more staff in monitoring software. So, training the staff is extremely crucial because they should be aware whether the attack has happened, what type of attack it is and how they should react to the attack. They created an incidence response team and practiced a simulated attack. So, they actually had talks about an incident response team to be instituted earlier, but they did not implement that, which was now implemented.

They retained a cyber security consulting firm and they instituted third party security audits. So, now as I mentioned, Ripley's recommendation was to disconnect all the production computers from the internet, rebuild the software systems from scratch and this would actually take a time period of about 24 to 36 hours to completely rebuild. So, obviously this had lot of confrontation from others and there were other recommendations such that one was building a new site from a new facility from the developmental files and later once the new site is ready, the old site can be switched off. So, now it is a time that we need to take a decision whether to go for Ripley's recommendation or whether to go for the resistance. So, now I want to ask you guys which you think should be the option that they should go for? Can I have like a raise of hands of those who think option 1 is better, for option 2 ? Okay.

So, can we have reasoning why you think option 1 or option 2 is better? If you go with option 1, there will be a shutdown of minimum 24 hours to 36 hours of the business, but with option 2, even though building a new site is an option, the existing site will be up and running, so the business continues. So, when we shift to the offshore new site also, there may be slight delay in the business, but it may be up and running with the new site. Okay. But again it is not a question of just the time you want to see the technical viability and the cost.

Okay. Yeah. Okay. So, one consideration is time, the other is cost. Anyone has any other comments to make? Just to add to the cost perspective, with option 1, for the time duration which it is shut down, there will be no sales coming in. And that timeline could

also extend based on how it is being implemented. Option 2, there will be additional cost where we will have more visibility, but at the same time sales will continue to come for that duration.

So, from a financial perspective, option 2 seems better. Right. Maybe we can have, I would suggest maybe we can have a moderated option to saying that we will know, because with every passing minute, if we keep the old site running up, we will be obviously facing some secret issues which we are unaware of as of now. So, what we can do is we can start building the new site and later when we have a kind of certain visibility that this site might lack some "t" hours and at that time after getting that visibility, we can switch off this later site. I mean, I am not saying that we need to switch off the old site only when the new site is built, but maybe sometime in the transition, in the middle so that we can ward off the risk from the old site.

Okay. So, yes. So, we weighed the pros and cons of both the options. So, with respect to option 1, the advantages is that it is less time consuming and the process is well documented, though there would be some expected time lag and it provides guarantees with respect to the files. However, the disadvantage is that it degrades customer satisfaction and when it is in very stiff competition, it is one of the top two players. This is the time when they actually want to gain profits and grow and at such a crucial time, they will be losing on customer sales and getting into increased competition. So, with respect to option 2, the advantage is that there will be no loss of sales and the new site will be free of all vulnerabilities because it is being rebuilt.

The disadvantage is that it is going to be extremely costly to obtain space in a hosting facility and in new equipment and keeping the old system live can actually have, can still be prone to other attacks which they are not sure of and building a new facility and new equipment will actually be more time consuming. That is what we feel and it is mentioned in the case that to come to normalcy, it would take about 3 weeks. So we feel that we are going for an option which is not exactly option 1 and 2, a middle ground, where we are suggesting that the server, a parallel server should be running and until the issue is being fixed in the original server. So when today's class we also saw that there should always be a parallel server which he mentioned that as hot site. So this parallel server can be turned on, if there is any issue with the original server.

So this should be done and one important thing is so far they have never taken any steps to diagnose the source of the issue. So this also has to be implemented. So moving on. Can I ask a question? Yes. So your solutions, your options you created are quite fine because that is a debate that is there in the organization.

So some are opposing this shutdown for one to one and a half days and instead suggesting that well, build a separate site but run the business as usual. So that is of course advantageous because nobody knows, business got disrupted. But the concern is coming from the technical person. You can see Ripley is just not satisfied because you don't know. And I think the specific problem here is that they examine the files and all files are there.

For example, file names are correct. That is checked. But they are not sure if the file contents have changed. Yes, exactly. So in that case again they are not sure there was intrusion.

There was actually new files installed or old files, existing files, tampered. They do not know. They only know that all the files with the same names exist. And since they do not know and since the attacks stopped on its own, the technical person feels that it is still unsafe. And then you say that we will build a parallel site say in a few months time.

We do not know how long it is going to take. Till that time what happens? Another attack can come in and it can be much bigger embarrassment for the company. So this is the scenario. So the moment you say that I am going by option 1, sorry option 2, you are saying that we are just ignoring what happened. We will just build a new site and keep it ready whenever a future attack happens.

But what is the guarantee that an attack will not happen tomorrow? See the hackers are smarter than the CIO. See the hackers are smarter than the CIO. Actually we have those recommendations at the end of these presentations. After the case. No, no when you stand at this point in time.

See the thing is that with more information you can do more things. But when you stand at the end of this case, all that you know is well what has happened and this is what you have in terms of systems and what you should do further is based on the information at this point. And a technical person would say well, if it attack happened yesterday morning it can happen tomorrow or anytime. And somebody stopped it on one's own.

So you are not sure. And that is why they insist on the recommendation, shut it down, do a thorough examination. That is why we also mentioned here that they should diagnose the source of the issue by conducting forensic audit etc. So this would actually bring them to a better situation. But that requires shutdown. That requires shutdown which the other side is opposing saying that well, let us not do that because you lose customers.

That is the, you are between the what you call the sea and the devil, right. It is a catch 22 situation, very difficult situation. Okay, you are going with one option. So moving on

part C would be taken over by Lokesh. So again now in part C we will see the sequence of events.

So first thing the senior management has decided not to shut down the business for a comprehensive rebuild of all the production platforms. And then the second step what they do is they have accelerated building the new site with whatever the available resources and instruments is currently at the site which is not affected. After 2 weeks there is an incident, there is a call from an FBI agent saying that the iPremier is attacking their competitors. And the source is from one of the, one of the systems which is inside the iPremier company, it is in the production site. So what happens is only then they go and check the file and they kill the file.

So they say that that is when they recognize that the firewall has been penetrated. And they also assume that the hackers have misdirected their attention saying that since it was in suspiciously it was stopped, the attack was stopped and they did not receive any further requests. So they thought that the attack is over but they did not expect this type of attack to be done. So it is the attacker, so the hacker, it is called as the suppressing the fire during the retreat. So now we see the after these issues when it has gone to an catastrophic level, so there is 3 issues the company is facing.

One is to implement the Ripley's recommendation. So if you go by that, if you initiate at this stage, it will be an, it is a source of an illegal attack. So if you start rebuilding it then FBI will be obviously suspicious and you will be almost destroying the evidence or whatever or you might, the evidence of, although you are not attacked it will still be shown that you are the attacker. So if you do that this is one of the issues. And then the second issue is how to handle the situation between the iPremier and the Market Top.

So definitely Market Top, the company is going to file a lawsuit against the iPremier. And here the question is how the iPremier will approach and what they are going to say to the Market Top to convince them or to get them on the like, on the same tracks of understanding. And also there is another issue on what they have to say publicly. Their database server has been compromised and also they could not identify any potential or significant individual customer who have been affected and in either they are not sure whether the data cards numbers or the credit card numbers are stolen or not. They are still in the dilemma and they are also perplexed whether this could have been happened or not.

So that is the other issue. And if they, if the credit card data is stolen then also again there will be an lawsuit filed for the violation of the credit card processing agreement. So now coming to the Ripley's recommendation, so do you, any of you have any suggestions

on what you should do further, or what to do with the options available? How the issue can be solved? It is theoretical. So run the services from a parallel Qdata server. Since they are the, they are the third party services which they have provided, so we can suggest them to give us in separate server and which could be fixed immediately by all the development files we have and keep the site running. And during that development site we, since it is an e-commerce website, so we can allow the customers to surf and not make any credit card payments until the issue is fixed.

And if the product is really needed at any emergency like within 2 or 3 days, they can go for a cash on delivery. So that is more safer rather than not giving the credit card details. And then how to handle the situation between the iPremier and the Market Top? So here is the question of an, the trust between the iPremier and the Market Top. So we can request the FBI to conduct a diagnosis at the iPremier our at the iPremier company and share the report with Market Top. So that will create a sense of trust and also evidently that iPremier is not the source of the attack, although the attack is coming from another site, the zombies which they call.

And they can collaborate with the Market Top and also they can build an security, ensure the security for their businesses like both of them, they both of them could be benefited if they come together. If not, they will be filing a lawsuit and both of them will be in the like, they would create an public attention and both of them would give an negative impression from the customers and both of them would lose their market shares. And what to say publicly? We say that, publish the incident report and the countermeasures taken. So what has happened from the start of the event to the end of the event and how they have tackled it and published their current incidents report whatever they have done. And then on the site we can, since we are not allowing them to make any credit card payments immediately, we can flash a message saying that the services are under maintenance and take a time to fix the issue.

So this is the one of the solutions we are providing. So any of them have any concerns with this or any countermeasures from your side? Thank you that was very enlightening. Sir apart from what they have told, so even if you start off with a parallel server, there is no guarantee as the same attack will not happen on that server and that server will not be able to prevent the same. So the question comes that how do you prevent it? So there has to be, anything which is connected back to the internet and it goes down, it will go down the same way. They don't have an answer for this, they could understand the impact also and it is likely to be the same in the next scenario also. So how do we do that? In this thing, the only probably the critical part was the credit card information and banking information, so the aim is to separate that from that particular server and I think the solution lies in that that the financial information which is there needs to be segregated

and should not have a direct access with the digital platform basically.

So there in comes that maybe it requires a more analogous method of keeping record and there has to be some kind of human interface, which has to intervene over here. So that even if the next system gets breached or any other system you can connect in any number of systems, you can have any amount of firewalls in this thing. If it is connected to this digital platform, it is likely to get affected. So human interface and more analogous means maybe the answer to protecting this.

So before going to like I can answer that but after. No, it is not a question. After two slides, we will provide you more detailed recommendations. So before going to that, we have two incidents, recent incidents which is taken currently. So one is the Microsoft services which has been affected now in the last two days previously. So they, what Microsoft immediately they did is they report, they went publicly and on the Twitter handle, they published that they are facing this incident and we are going to fix it and also they are given an updates on each time what is happening.

So that creates a sense of trust among all the business and almost all the business are dependent on the Microsoft teams and the Microsoft services and here there is a report saying that the major affected services is the Outlook and their website and then the Excel and the locations are highlighted probably it is not visible, I guess. Those are Bangalore, Chennai, Hyderabad, India, Nagpur, Mumbai and Delhi. So these are the locations which are majorly affected and now the businesses, it has to keep running on. So what they do is they go for this, they are told that they have isolated the problem to network configuration issues and we are analysing the best mitigation strategy to address this without causing the additional impact and within two hours, they were able to fix this issue and the services were on.

and the business were back. Now here in the next slide we will see how the businesses and the employees have been reacted. So here one of the maybe,the employees so they took a vacation. So they say that Microsoft teams has stopped working which means that work has stopped. So it is a kind of break for them but they did not like, what you say they did not have any other issues, they just needed a break so this two years gap, it was a break to him. And then there are few other responses, for privacy we have blanked it out.

So it says, come on it is up now why did you fix it so soon ? The days when exchange was on prem were better at least the outage used to be for few hours but they fixed it within 6 to 9 minutes. So they were very well advanced and they had a good protections and the firewall updated and since because of that they were easily able to fix the issue

and there is another response which says that thank you for the service down, spent all the day solving the issues for the full box, inbox and enterprise plan and here you see he is ready to move to Google for an one TB plan. So Google is also one of the email services, Google and Microsoft they provide and it is still a competitor. So they are ready to move to other plans if the issue is not fixed in a quicker time and also you can see that the stock at the time when the incident was reported, the Microsoft stock has dipped for almost 20 USD dollars. So this is the kind of impact a business can have when such incidents it occur in the real scenarios.

And next we see one of the major cyber attack, the DDoS attack which Google has faced. So on it was in the last year on June 1st, 2022 the cloud armor customer was targeted within series of HTTPS attacks which peaked at 46 million response request per second. So how they tackled this, they had a tool called as cloud armor adaptive protection, it was able to detect and analyze the traffic early in the attack life cycle and it blocked the attack ensuring the customer service stayed online and continued the servicing their end users. So they did not shut down their businesses they let the customers, their businesses and the other customers to be online and they did not affect their usage. So there were, as our widgets are told there should be some functions which should be like segregated, so here one of the function is they allow them to stay online and use these certain services but the back end they were fixing it.

So how the attack was stopped - one is the rate limiting capability to throttle the attack. So here the rate limiting, they had an protection and they had an rate limit saying that their server could accept only 1 million request per second but here there were 46 million request per second that is how they detected there is an breach and they controlled it. So by, they were already aware of this attacks which is happening and they controlled it. So what happens is, here the layer you can see, the 7 layers which is mentioned. So the third and fourth layer is the where the infrastructure layer is getting affected and the sixth and the seventh layer is the application layer based attack.

So here the Google were facing an infrastructure layered attack so which is on the third and the fourth layers and then they had an depth in depth defence in depth strategy. So which means they had to control, they had a different controls for each of the layers so they did not have an as a package, they did not go on single for each for a like one layer there was a protection and that is how the hackers were able to attack the third and fourth but not the other layers. So here they also had the threat modelling that is practicing the attack and as we saw that red, blue and the purple strategies. So they practice the threat modelling and that is how they come, they build their own practices So here they had an proactive and like they had a two options proactive and reactive strategies but they were not reactive in this case it was a proactive strategy which they have used. So this is the

case we have gone through and now we go on for the recommendations.

So before that any questions? Yeah, this is a really good current insights you have brought to the analysis especially about Microsoft and Google and how they are really transparent and competent professionally competent to face cyber attacks and which is evidenced in public but the only small issue is you are jumping out of context. So here are two technology companies, that also world's top technology companies who are competent, technically competent and then comparing it with a non technology we cannot say non technology company but their primary business is retail. But they have IT assets which is managed by a third party Qdata and Qdata's competence is questionable, that is what we discussed in the last class. So in fact for cyber security they are dependent on Qdata whose data center is not equipped with the state of the art cyber security technologies. So even if they build another site, the primary requirement as somebody suggested from the audience is they should have updated firewall, they should have updated intrusion detection systems and only then they should migrate, otherwise there is no point because you know, they are again vulnerable.

So that is again another investment and another decision that the company has to take. So these are basically, it is like comparing apples and oranges but fine, it gives some updated information as to how, what is the professional practice today versus what the company is actually struggling with, no strategy for cyber attacks at all. So we have recommendations. Yeah so, for there are so many mitigation techniques, this can be preventive, detective or reactive and mostly these are technical mitigation techniques that we are suggesting and first one is to reduce the attack surface area that is by limiting the option for attackers. As Sir had discussed today, there will be vulnerabilities no matter how much protection you give.

So to reduce that is the first option and there are content delivery networks or CDNs which what happens is when a huge number of packets come in and there is unusual traffic, these CDNs will distribute this across many multiple servers that are lodged in the internet and this will reduce the, you know, server traffic at one point of time. So these CDNs are used by almost all the leading companies, e-commerce websites like Amazon etc because they are constantly attacked by DDoS and these CDNs will help reduce the traffic at one point of time and second point is knowing what is normal and what is abnormal. In iPremier company what had happened was abnormal amount of traffic during non-business hours, that is when everybody was sleeping. So that had to be, you know raised as an abnormal activity which was not done by the Qdata as a architecture and next is plan for scale and their servers were not capacitated enough to entertain that much amount of traffic. So we have to have load balances and shift loads when such amount of traffic happens.

So usually what leading companies do is they have DDoS protection services. In 2018, when GitHub was attacked by a malicious DDoS attack, what it had is a Akamai Prolexic which is its DDoS protection software and this effectively, you know, tackle that DDoS attack. So they can also follow that suit and they have to deploy firewalls for sophisticated application attacks. There are different kind of firewall and it depends on the cost that you invest, the protection the firewall will give. So there are packet firewalls, there are MAC filtering firewalls and there are hybrid firewalls. So as we go more advance, it will give protection against all the vulnerabilities.

So they have to go into firefighting mode and invest in these kind of firewalls to you know, see if there has been change in the content of the files or there is any potential for future attacks. So they have to invest in this. So these are basically management side reactive measures. So they have to invest in this.

So these are basically management side reactive measures. So once an attack happens, what they have to do? So this CIA is the basis of cyber security, in this the A that is availability was not even there in the first place. For example, Ripley did not have access to the Qdata server and they were not letting her in, when the attack happened. So that should not be the case and our suggestion is that they move to internal IT team, so that these kinds of incident do not happen. Then there has to be DRP, IRP and BCP which was not in the first place.

So IRP is something that they do during the course of the adverse incident. DRP is the disaster recovery. So after the disaster has happened, what are the recovery steps that needed to be done and BCP is as we have said, run the process in a parallel website. So that was not there and that has to be implemented and the hardware and software needs to be updated. For example, there are so many DDoS protection softwares that are existing and being used by all the companies like there is unified threat management devices, UTMs then there is express data paths. So all these can be implemented by them as well and the roles and responsibilities had to be adhered.

For example, when this attack happened nobody knew whom to contact. They were not even in a position to go for a conference call and have all the options being considered at one point of time. So they were confused as to what to do. So as NIST suggests, there is a 7 step contingency management plan that is mentioned in the textbook as well. So there is a contingency management committee, management team which is CPMT and there is a champion, there is a project manager and there are members. So this CPMT team has to be formed in the first place who will be the first responsible if such an attack happens.

So as Sanjana said, the first thing is to be identifying the source of the attack and immediately forensic report has to be recorded and maintained and finally they can also go for a parallel server in which they can keep the business running if this stops. Thank you. Okay, thank you. Thank you.