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: 02
Lecture: 06

Let us come to the second question, I will give you a summary in the next few slides. The second question is about the impact, what happens? Well, there is an incident, despite all the investments of the company in cyber security, a major incident happened, but what, how do you actually assess the impact of it? Can impact itself look at tangible or measurable or quantifiable impact? You want to answer? Yeah. Yes, as in this case we can see that it has various impacts such as monetary impacts with various stakeholders such as banks, credit unions and people and businesses . Credit may not be credit unions, but credit card companies. Credit card companies, payment providers. Credit unions are different, we will discuss later.

And as well as the government institutions as to. Which ones? Government. Government. As compliance policies and it was a watershed moment in the cyber security.

All got affected, but are there some measures of how much was the impact? how much was the loss? So in total, net total it was around 100 million US dollars. Okay, 100 million dollars and where did the company have to spend this money on, where did, how did this go out? Like, it went partially to banks and 10 million to people and it was from insurance companies, it was a pay out of 90 millions and for like credit payment providers like Visa and it was settled for around 20 million dollars and for banks. So there were individual customers who sued Target, they were also banks and credit card companies which actually went to the court. So actually you can imagine this company which is doing very well, Target, beautiful when you go out, very spacious retail outlet. So people love to go there and shop and you must, some of you may have shopping experience, but all of a sudden what happens to the image about the companies? Well I lost my, lost my credit card information and that credit card or my bank account details has now become vulnerable.

And therefore some customers can go to court and that is what happened and then of course there has to be settlement of that in the court where the company pays fine. So that amounted to a good sum which is 100 million US dollars. So that is a tangible. What do you think about the intangible aspect? Along with tangible loss, there is also intangible

cost. Like sir, as far as this intangible is concerned, like the trust of the customers you know that has suffered, the reputation of the company that has suffered and also the opportunity cost is there.

That business what the company has lost actually. In accounting you have a word, goodwill. Goodwill loss is a major loss. Customers may go to Walmart now, not to Target. So I, you know I, once your fingers are burned, then you would not actually try that again even if they take a lot of positive steps at least for quite some years, you may not go there.

So that does happen. So all of you have experiences stopping business with certain businesses because of bad experiences and then you do not go back. And for this company, goodwill is very important because retail space is very competitive and you have equally good shopping experience in other places in similar locations. So why should someone go to Target? So they very much care about it. So the goodwill loss is a major impact.

So let me actually take you through my slides and these were your answers and you have attempted well. So let us together understand and wrap up this case of Target Corporation which gives us, is there anything that you want to add? Yeah sure. The previous slide. The previous slide. Questions.

Okay. So another intangible impact from my point of view was that it also affected the, it also made the government to rethink about how they were framing their policy regulations because a paragraph was mentioned in the article saying that, they already had few policy regulations in place but they were not properly framed saying that in this case Target had also had to repay customers whose data was not actually damaged. They were breached but they were not damaged it seems. So in such cases, it also affected the stakeholder's reputation from customers point of view as well as from government's point of view and they found that there is more need because a significant proportion of their population, obviously, their data is located in such retail chains as well. So they found that, in such case of a breach, they had to redefine their policy framing regulations in order to take care of such losses in the future as well. So that was another intangible impact post which, there are a lot of policy regulations that came into play.

Okay, so how to address data breach instances and who is responsible and how much you pay as fine. Okay, so all these are actually matters of regulation as well. If there is no law against privacy or data breach, then companies can continue to do what they do but unless the law requires them to act responsibly, there will not be redressal of these issues. Also sir, we have to see the role of chief technological officer or the CIO, chief information officer and how they have to act in a strategic measure you know, to conduct the training and the awareness of the employees. Okay, towards the cyber security

measures.

Okay, this is about government policy, this is about company policy. Yes, internal. Okay, so you know this is in terms of action taken or in terms of reflection of what went wrong and what needs to be done further. So that was actually the effect of this incident on, you know, some stakeholders like the government, like the top management and so on. So let me actually summarize this case with the help of slides so that you know there is clear understanding of what happened and what could have been done to prevent and what was done actually to prevent subsequently and what are some of the open questions now.

So, as we saw in 2013 this happened during the Christmas Thanksgiving season and Target has 1797 US stores, it is a large corporation and Target was actually technologically very updated, you know as we saw that in the beginning. The company had huge investments- 1.6 million malware detection, dollar 1.6 million malware detection tool was installed six months back. So why should they actually face such a problem despite having this investments.

Okay, so it used the same security system as the CIA, not the CIA triangle which we discussed but the CIA, the intelligence agency of the United States. So it is like, they are they were very updated in terms of protection mechanisms like the, like the government. So they had multiple layers of protection, we have seen all this and they also had periodic audits like the external validation , benchmarking assessments, all that was done. So people and processes were also in place for Target Corporation and they complied with data security standards in the credit card industry, everything is being done. So that is the case often times, you do whatever is required for regular compliance but incidents happen still and you can say, they are still happening, you hear about data breaches in recent times as well.

Despite this happening in 2013, organizations still have data breach issues. What really went wrong as we said, hackers gained access to Target systems through a vendor's access which was not defined correctly. And of course, it failed to segment its network to ensure that third parties do not get access to the POS system, that was a failure. Can we can call it techno managerial failure? and that is what hackers exploited, as I said in the beginning. And so they actually used this connection to upload malware into Target's systems and what happens, that is the exploit.

So the malware used by hackers was programmed to steal Target's customer data from the point of sale. And the real vulnerability, the technical vulnerability, was the problem of encryption you know which was exploited using RAM scrapers, which is the particular

software they installed in the POS system, to tap data from the POS system, RAM scrapers. And we discussed the impact. Customers and banks have filed more than 90 lawsuits as the case suggests and in numbers, Target's profit for the 2013 holiday shopping period, fell 46 percent. So there was an immediate impact, financial impact which is the loss of revenues during the peak period of shopping and in sentiment or in goodwill, they lost the goodwill of customers, investors and lenders.

Now, let us look at it from the administrative point of view. So this is like the Titanic. So you are running a ship, you are the captain of a ship and for a captain, of course, taking you to point A to point B is the objective and taking you safely is the real objective. But so therefore, safety is critically important to the leadership of cyber security, cyber security management. So you can see that in such a context, for such a reputed organization somebody switched off the malware reporting system, which is actually safety.

So somebody compromised on the safety. Have you watched the Titanic? and you know the Titanic, this is Titanic is historical, right. What went wrong with Titanic? There is research done on this, on Titanic. The movie is, of course very nice. What was Captain Smith's error? You can take a while to recall.

You know, it was Captain Smith's last ride, he was going to retire. And he had a smooth sail. The sea looked very calm outside, you know the blue sea people are having fun, they are having good time, enjoying the time enjoying the ride ,sea is calm, his last ride, everything looks fine. And then he started getting warning. Warning from nearby ships that there is a iceberg and Captain Smith apparently looked outside and how can there be an iceberg? Everything looks fine, the sea is calm.

So you cannot believe when this riding is smooth you tend, sorry for making it dramatic, it may not be exactly what happened but everything looked safe outside, apparently everything looked safe outside. You know from history that he did not act on that warning. He ignored the warning and went for a cocktail, that is the story. So if a captain ignores safety warning, what could happen is the historical example of Titanic. So here is it from literature, as to what happened.

He was over confident for too big to fail. Yeah, good point. He was over confident, the weather was calm and clear and it gave no perceptible reasons, you know, mind can be very deceptive. So everything looks fine, like I look at the class, everyone seemed to be fine and enjoying, but do I know if you are learning. I need to actually conduct an examination or actually make it a little more objective or scientific to rely on what I perceive.

Perceptions can be good, perceptions can be deceptive as well and it appears that wrong perception, played a role in this Titanic incident. And that is a warning for actually managers. So, since it is a beginning of the course and this gives a management direction for future practicing managers who are related to cyber security management, attitude does matter. As managers you are responsible and any safety warning, any warning that is related to safety, should not be ignored. We all fly aircrafts, we all travel in surface transport, be it trains, be it buses and systems have been put in place, to ensure that your journey is safe.

Well, what do you think is the most safe transport mechanism- is it road transport, is it train or is it flight? Is flying more safe or buses more safe or train more safe? You have read about it or it is your, you want to imagine. Statistically. Your answer is correct, actually flying is the most safe. Based on data. So you can imagine the extent of effort and there are very strict protocols and they follow the protocols and nobody would, unless someone goes out of mind, you have some incidents like that, you know a pilot flying a aircraft to, you know, into some mountain and killing everyone.

So there are rare incidents but otherwise these are all safe thanks to the protocols and thanks to the safety mechanisms built in and if you bypass that you are actually, you are the captain of Titanic. If you are actually bypassing safety. I strongly suggest Andrew Grove's book, Only The Paranoid Survive, for managers. This is an old book but you, in management talks, you actually come across several terms that he coined in the book - Inflection point, 10x force, he modified Porters five forces and said if one force is 10 times others, what should the manager do, you know, very insightful thoughts. And the key point in the book is, you know, be a paranoid, doubt everything.

You tend to think that everything is going fine and you want to believe that everything is good. Because the managers just do not do it. You worry about everything. He said, I worry about plants, I worry about people, I worry about market, I worry, you know, paranoid is a negative word, you know, that it is very negative but it is a sort of the attitude that he tried to build, when the competition was very high and it took decisions which actually led or show correct directions for Intel particularly, signing out of the memory chip business and so on. The book is very, very useful for managers.

Of course, it is a bit dated but for cyber security, I would say paranoid mindset is a very important mindset. Look specifically, at the case of Target corporation. I just want to bring to your notice some important takeaways. Number one, lesson on employees ability to circumvent security. So one key learning from this incident was that despite huge investment in cyber security, if managerial processes are not foolproof, there is no point.

All that investment do not make sense, if there are vulnerabilities in management. So importance of management in cyber security got more highlighted after this incident. We have security systems or security technologies like the CIA but what happened. So that is because of administrative failure. Number two, as the case says it was a watershed moment for cyber security regulation.

So there are several laws in the US. We will be exploring the regulation or regulatory landscape in different regions in the course But despite that, there were lack of clarity in terms of what needs to be done when there is a breach, how it should be reported , what kind of redressal mechanisms should be followed etc. So there is no one comprehensive regulation for cyber security and privacy in the United States. European Union has it, but it is still evolving in US, even today. Number two, we looked at the tangible laws and we found it is 100 million and look at the size of the company - a 72 billion, that is the revenues and you lose 100 million from that, it is like a pickpocket, you know, somebody stole 100 rupees from your pocket, How does it matter? So one advice ,we will see in cyber security management, there are different positions a management can take in cyber security. You can ignore this altogether and we will face this in the court.

We do not want to make huge investment in cyber security. If there are incidents, we will see in the court. So when a 100 million loss, it does not matter. So one industry observer said that is a quote I have given, as long as the fines are not putting business into bankruptcy or even serious financial parole for that matter. Executives and boards are free to decide they are better off investing the bare minimum in a security, in security and saving the rest for possible breach cost and fines.

So ignore the warning, is another management position. What do you think about it? Is it a good stand? Can companies choose to invest bare minimum in security and face it in the court? So government as a regulator or government as a body which wrecks the interest of people this may not be right but companies can make a choice in the absence of regulation. Well, they will comply with the law if there are incidents. For example, you lost some money, I will compensate, I will pay fines, that is fine but we do not want to create such large system for cyber security. So it may also be influenced by the extent of competition in the industry because if some players put in more security, customers will have more trust in those and automatically everyone else will sort of be forced to enhance security.

Yeah, that is a valid point perhaps the intention of Target, in making huge investment in cyber security was also to signal to the market, well, your data is safe with us and we have invested so much in cyber security, you are safe. But despite that, of course the incident did happen but your point is, if you do not do that, if you do not invest and signal,

it may affect your reputation in the market and it may become a disadvantage in the market which is correct. You can see that, that is why probably the company has made that investment. So shying away from that, may not be the right choice in competitive environment.

Good point. So we will see when we discuss risk management, cyber security risk management what are the options available to decision makers in cyber security and how those options can be exercised ? Okay, it is like some of you decide, oh well , I do not write the examination or I will repeat the course. So it is like you know I do not, I am busy now but I am making an informed decision, well, I have a plan. It is not that you are just closing your eyes against safety hazards but you have a plan, if it goes wrong, I have a plan, well, I will write it later. So that kind of an informed step is potentially possible and that is being done also. So we will take that up as a separate discussion in risk management later.

Any questions? We are done for this session but if you have questions, we can discuss or we can close. Okay good, so we have an introduction to cyber security at a fundamental level, the CIA - confidentiality, integrity and availability and mechanisms to ensure them and we also discussed a case where you see, how security breach, data breach did happen, despite efforts by the company to secure the cyber assets. And we are learning certain lessons and we will refer to this case again when we discuss, more concepts in the coming days. I will see you in the next class. Thank you very much.