Information Security – IV
Prof. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 03
WISE GEN – Next Step

Welcome to session 3. So, we were actually discussing a vulnerability information security leak that happen, because of a photocopy machine, and that was basically found out by Wise Gen; the heroin of the story. If you look at an infrastructure I T infrastructure, when you want to build a secure I T infrastructure where in you can do the forensic in case of an attack and you can also protected so that there are no attacks, two parts one to protect it.

So, that does not attack and in case of an attack how effectively can I do forensic, both of this involves that I need to select the hardware properly, I need to select the software properly, I need to also select the vendor properly right.

(Refer Slide Time: 00:50)

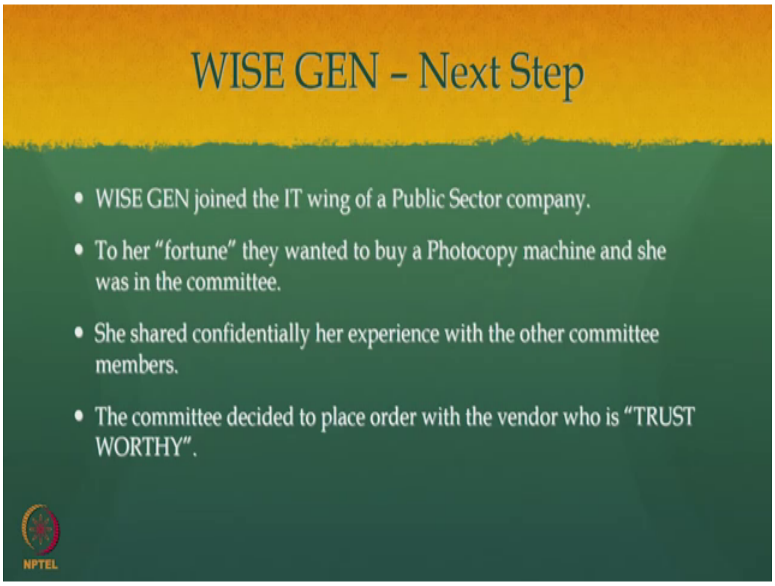
IT-head Responsibilities

- Hardware Selection
- Software Selection
- Vendor Selection

- Gave a clue on Hardware/Vendor selection
- Can I continue with my story?

I will give you lot more examples of how each of these are very important right. If you have a tricky vendor, we already saw one example, if the vendor is not a trustworthy vendor, you may loos, and that loss maybe very significant, it can even do it lead to the complete processor of the company please note that. So, I will continue with that story, a hopefully you are liking this. So, I will continue with the story. After the debacle act T T T, the T described in the last two sessions by heroin Wise Gen.

(Refer Slide Time: 01:36)



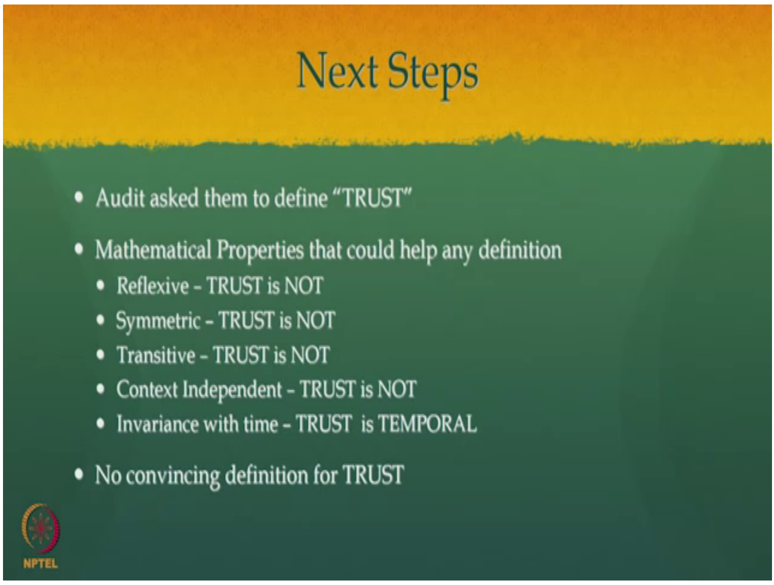
WISE GEN - Next Step

- WISE GEN joined the IT wing of a Public Sector company.
- To her "fortune" they wanted to buy a Photocopy machine and she was in the committee.
- She shared confidentially her experience with the other committee members.
- The committee decided to place order with the vendor who is "TRUST WORTHY".

She joined the I T wing of a public sector company, and to her fortune quote unquote, they wanted to behave photocopy machine and she was made member of the committee. She shared very confidentially her experience with the other committee members, because if she make it public, that J K L will sue for a defamation case. She went and confidently told a in the previous thing this happened, so let us speak out very happy.

So, this is also very important today; like when a fraud occurs and your forensic cannot established that that fraud has occurred, but you know that this is the real reason, this reason cannot be publicly told out right. So, though this is a real reason but if you do not have the proof that this is a real reason right. This essentially, even if there is a small there is no doubt that this is the reason, but then I cannot prove that this is the reason. So, that was some very interesting example that we saw in the past, in the last two sessions. The committee actually decided to place order with the vendor is trustworthy.

(Refer Slide Time: 02:53)



Next Steps

- Audit asked them to define "TRUST"
- Mathematical Properties that could help any definition
  - Reflexive - TRUST is NOT
  - Symmetric - TRUST is NOT
  - Transitive - TRUST is NOT
  - Context Independent - TRUST is NOT
  - Invariance with time - TRUST is TEMPORAL
- No convincing definition for TRUST

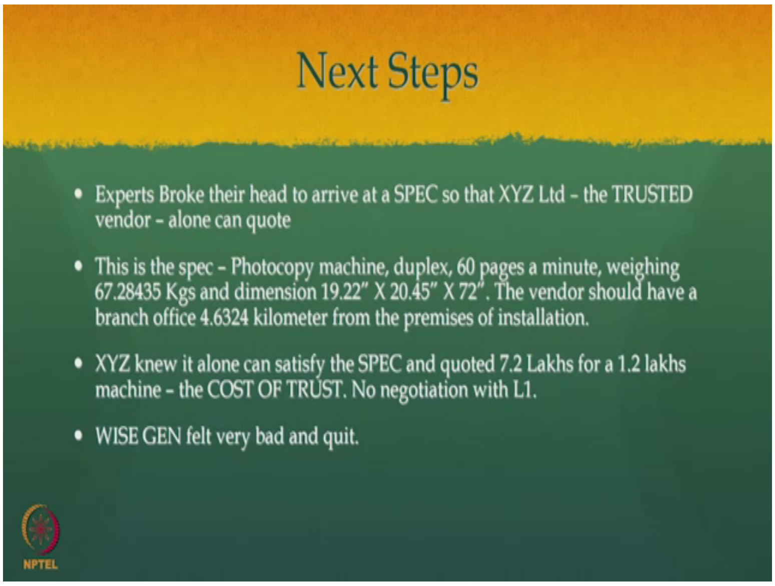
.

Now, this is something that I covered in the first information security course; information security one, three has before a court is trust. So, when this went to file went to the audit, because the public sector there is an audit, the audit committee said what do you mean by trustworthy and define trust right. So, I hope many of your computer scientist, even I will take it, but just I will try and make it; if I want to define something mathematically, like I want to define X mathematically. So, there is a relation between that should be this X should satisfy certain properties. So, there is something called a relation is called an equivalence relation, if that relation is reflexive, if the relation is symmetric, if the relation is transitive.

If a relation is equivalence relation then I can actually go and make a good definition of that relation. Trust is also a relation, trust is a relation between X and Y, I trust that system meaning this relation between X and I myself and the system. Now trust is not reflective, sometimes I do not trust myself, many times I do not trust myself, trust is not symmetric. I trust A trust B, B need not trust A, trust is not transitive A trust B, B trust C, A need not trust C, trust is context independent. I trust you for something, I do not trust you for something else and trust is not in variant to time morning I will trust you, evening I will not trust you, tomorrow morning I may again start trusting you.

So, all the five properties which actually makes definition of any relation easy, namely reflexive, symmetric, transitive, context independence and invariance to time, all these five are missing in the case of trust. So, coming out with a mathematical definition of trust is going to be extremely complex. They could not come with a convincing definition of trust. So, they went, so audit said nothing doing you have to give me a definition of trust, these guys broke the head no. So, they cannot pushed up purchase; saying I want a trustworthy vendor. So, the next thing that normally happens, we have to buy that when that vendor. So, then we start giving them specifications; such that that trustworthy vendor alone can meet that specification and this is expect.

(Refer Slide Time: 05:23)



Next Steps

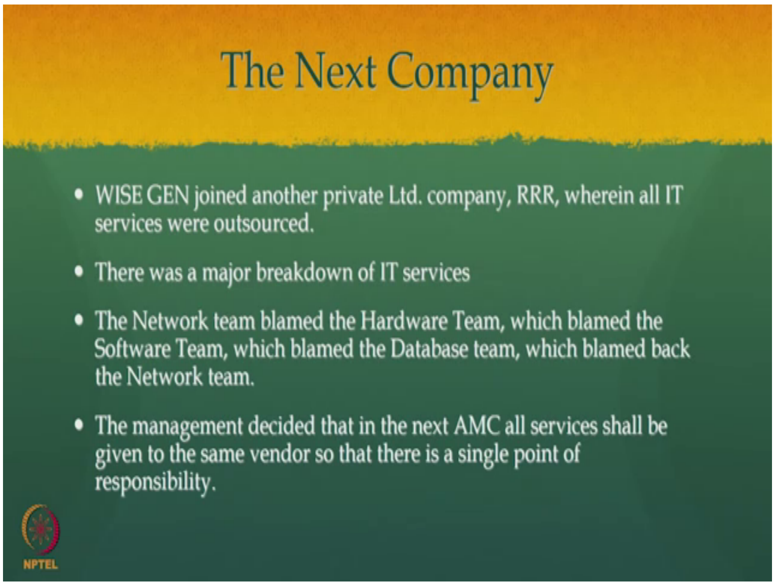
- Experts Broke their head to arrive at a SPEC so that XYZ Ltd - the TRUSTED vendor - alone can quote
- This is the spec - Photocopy machine, duplex, 60 pages a minute, weighing 67.28435 Kgs and dimension 19.22" X 20.45" X 72". The vendor should have a branch office 4.6324 kilometer from the premises of installation.
- XYZ knew it alone can satisfy the SPEC and quoted 7.2 Lakhs for a 1.2 lakhs machine - the COST OF TRUST. No negotiation with L1.
- WISE GEN felt very bad and quit.

So, I need a photocopy machine, duplex, sixty pages a minute, weighing some 67.28435 Kgs and dimension 19.22 cross 20.45 cross 72, the vendor should have a branch office which is 4.6324 kilometres from the premises of installation. This entire tender was put in such a way that, the person I trust basically quotes for me; otherwise the company will be completely endangered, the public sector company will be completely endangered. Now, the vendor who is coding for this X Y Z what were that vendor new that this spec will only meeting. So, instead of each (Refer Time: 05:59) instead of quoting say 1.2 lakhs he went and quote it 7.2 lakhs, 6 times (Refer Time: 06:04) because you knows nobody else can quote and this becomes the cost of trust today right.

So, there is very important. So, all processes are followed, I need to buy, I cannot buy some tom dick and harry and invests this, depending upon the previous experience which was jean actually told that committee. The committee cannot risk buying it from somebody else we do not know, they have any camera inside which can be activated through an internet or a Bluetooth or something and they can carry. So, if I cannot photocopy a particular confidential document inside an organisation, safely, securely, I do not think anybody can run the organization.

So, the committee was correct in basically telling that some of you have to get it from this X Y Z, who they believe that it is trustworthy, they need not be trustworthy, but this is fair. And the moment you start tailor making some of these things to suit that purchase, then the cost, this is the cost of monopoly here. If I know that I alone will win a tender then whatever price I quote becomes the benchmark. So, actually Wise Gen very felt very bad and she actually quit this organisation. So, then she went to a next company, this is a correct path which is some R R R, and then again that the complete I T operations outsourced, some days later there was a major breakdown of the I T services.

(Refer Slide Time: 07:24)



The Next Company

- WISE GEN joined another private Ltd. company, RRR, wherein all IT services were outsourced.
- There was a major breakdown of IT services
- The Network team blamed the Hardware Team, which blamed the Software Team, which blamed the Database team, which blamed back the Network team.
- The management decided that in the next AMC all services shall be given to the same vendor so that there is a single point of responsibility.

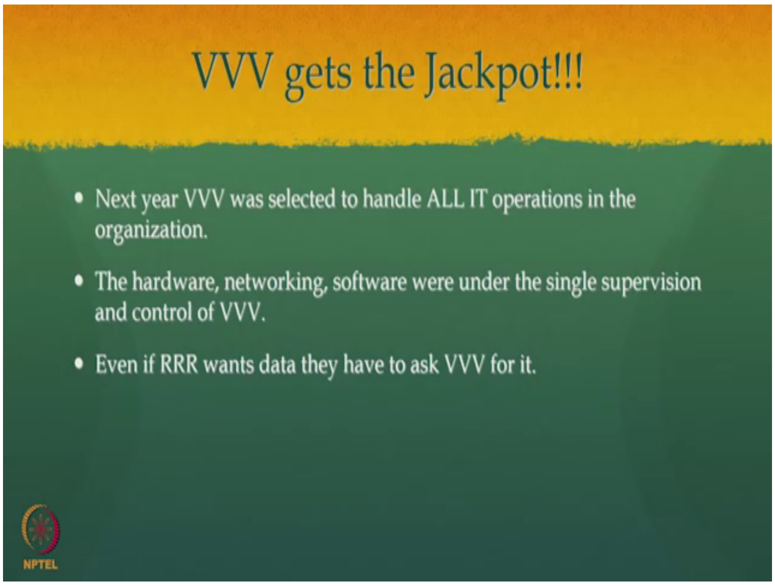
This is all stopped, when she went ahead and then looked at what are all the different components. So, there was a network team, there was a hardware involved, there was a software involved, there was a database involved, at least four different teams were working together run in the show. Then she will started analysing what went wrong in this whole thing, she found her that the network team blame the hardware team, which in turn blame the software team, which in turn blame the database team, which in turn blame back the network team.

So, this guys are going on a merry go round, merry for them, paying for others, for the company, because things are not coming up right. This is typically the scenario right. So, if; so I say that there is nothing wrong, he has given it wrong. So, I go AMC says he has given wrong and then people are just showing hands and this was just an entire I T infrastructure keep distance it.

So, the management decided ok. Please note the management decided that, this cannot happen each and each one will be blaming each one, and I will be suffering after paying all the AMC and other things, this is stupid let us put one fellow, and you will be responsible for all the things, you will be responsible for the network, he will be responsible for the hardware, he will be responsible for the database, he will also be responsible for the software , and if there is a failure; that is one fellow whom I can catch and ask him hey bring it up.

Please note as a process this is the best decision, and is an obvious decision that any management will take, if they are put into a scenario like what we saw. Now, the company V V V which got this entire contract, maintain everything for us, extremely happy, it actually got that J jackpot. So, V V V was selected to handle all I T operations, the hardware, the networking, the software under and you know all these under the single supervision and control of V V V.

(Refer Slide Time: 09:23)

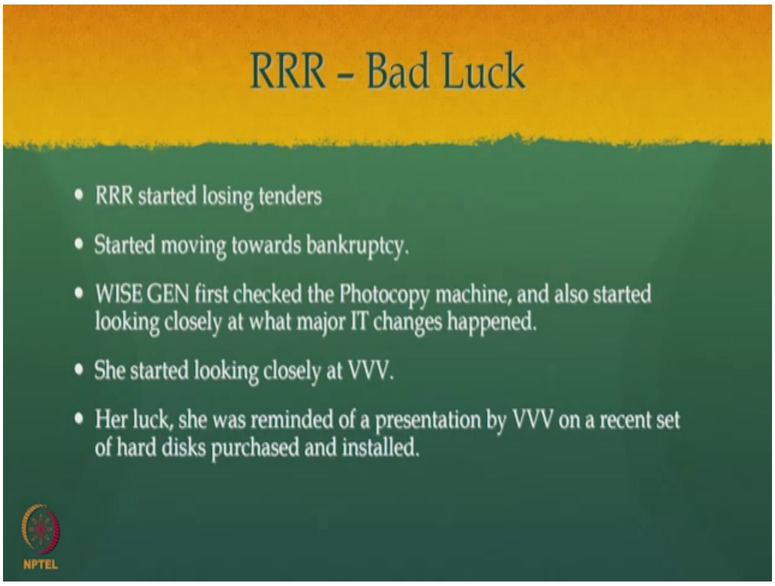


VVV gets the Jackpot!!!

- Next year VVV was selected to handle ALL IT operations in the organization.
- The hardware, networking, software were under the single supervision and control of VVV.
- Even if RRR wants data they have to ask VVV for it.

When it comes to that when I have a single fellow handling all these things, even if the parent company wants some data it has to go and ask that V V V and they will give the data. So, that is the sort of complete monopoly that happened. So, whatever happens in the database, in the network, in the hardware, in the software, everything V V V has a control over it, if he does not have a control he cannot maintain it.

(Refer Slide Time: 09:49)



RRR - Bad Luck

- RRR started losing tenders
- Started moving towards bankruptcy.
- WISE GEN first checked the Photocopy machine, and also started looking closely at what major IT changes happened.
- She started looking closely at VVV.
- Her luck, she was reminded of a presentation by VVV on a recent set of hard disks purchased and installed.

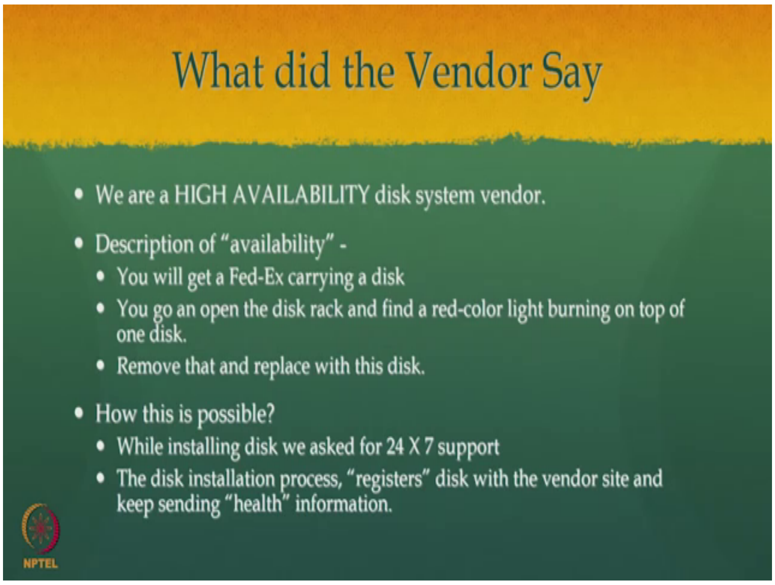
Now let us see what happens this company R R R again started having bad luck. He started again loosing tenders, and it started slowly moving towards bankruptcy, not as fast as the first company where Wise Gen worked T T T company, that you saw in the session one. Slowly this started moving towards bankruptcy, Wise Gen based on a previous experience, again I repeat she is a wise heroin.

So, she immediately went and checked the photocopy machine, if there a camera inside, then she started looking closely what happened in the last one year, it should be something related to I T, that I am again started losing tender, it is very similar to what happened in my first company the T T T right. Let us go and find out what happened here.

So, she start at closely, the only major change that was happened was in the A M C, instead of four fellows handling the whole show, one fellow is handling the whole show, he was handling networking, he was handling database, he was handling hardware, he was handling software. So, she started looking closely at V V V, and she started also praying god and luck came. Please note that many things come by share luck and here luck played a role, she immediately remember that there was a presentation by that vendor V V V was maintaining the A M C about a high availability disc that has purchased, high availability disc means it will never fail, it gives you 24 cross 7 cross 365 days, it will available always.

The failure would be point naught naught, naught, naught, naught, naught how many zeros, 1 percent. So, that is what do you mean by high availability disc, because finally, when you run many of these I T infrastructure, that data that is generated and stored is extremely important. So, if the disc files everything fails right. So, disc becomes the most important entity in this whole story.

(Refer Slide Time: 11:51)



What did the Vendor Say

- We are a HIGH AVAILABILITY disk system vendor.
- Description of "availability" -
  - You will get a Fed-Ex carrying a disk
  - You go an open the disk rack and find a red-color light burning on top of one disk.
  - Remove that and replace with this disk.
- How this is possible?
  - While installing disk we asked for 24 X 7 support
  - The disk installation process, "registers" disk with the vendor site and keep sending "health" information.

What was this high availability disc; so you buy the disc from a vendor. Now you are sitting in your office, suddenly one Fed Ex will come; Fed Ex is one courier will come, then you remove that courier then you see a disc inside, then you carried disc to the data centre, you open the rack, there will be one disc having a red colour, you need not shutdown or do anything, you just pull that disc out and push this disc, new disc that has come and the whole system will start running.

So, the failed disc is replaced with a new disc without disrupting the service right. So, this disc is actually called as, this type of disc are called RAID right, RAID means redundant array of independent discs.

So, instead of having a copy on one disc will have the copy spread across multiple disc. So, even if one files I can remove that one and put a new one and rebuild it very quickly on the fly without shutting down the system , and I will not loos any data. I also suggest people to who are listening, who do not know what is RAID R A I D RAID (redundant array of independent disc) to go and look at this technology and find out what happened there.

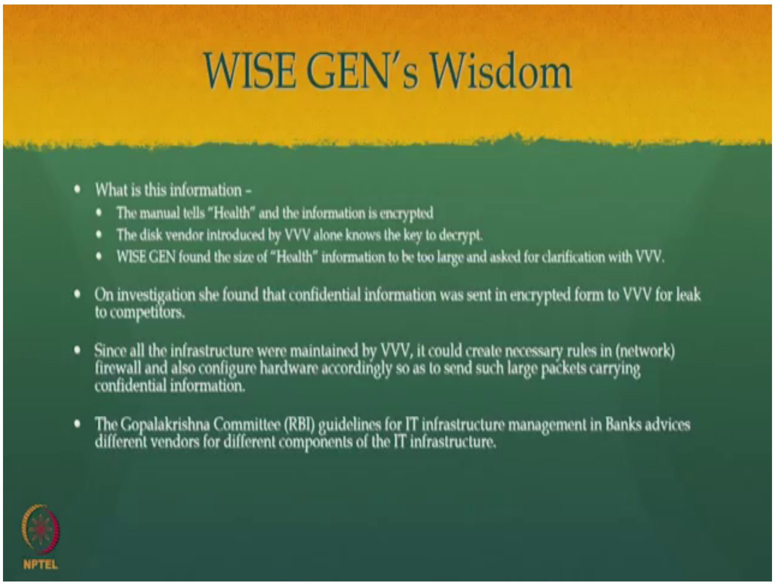
These are also called as hot swappable disc right. Hot swappable means when the system is running; I can pull out the disc from it and pushed a new disc and make the system run without stopping. These are all very important for I T infrastructure, if you look at some of the websites today, major trading websites or retail websites, if they even stop for some small duration the lose is phenomenally high went to millions of dollars that is, what they say.

So, all this service providers will have this type of high availability disc right. Now how this is possible in a data centre some disc went off put, I do not know what it is, even before I know the company whose manufacturing the disc knows it and he sends me by courier a disc, after I receive the disc only I come to know that the disc is failed, how is this is possible. The simple answer to this question is, that while installing the disc they will register for it 24 cross 7 support and subsequently after this installation and regular interval say every 5 minutes or 10 minutes.

This disc will send health of the disc, it is your own health information; like is there any failed sectors, how many errors came in the past, is there any voltage regulation issues, is that the spindles are working correctly or if it is S S D what is the number of time things have been erased, something called the health of the disc is important m and it will be sending it regular intervals and when the disc fails automatically this detail will be send there, and there will be some software which is looking at this and hey this disc has failed. So, whose disc is this is, this is the vendor to this address send another disc. So, all this decision could actually be automated and it happens automatically.

Now, Wise gen when then found out what is this health information; how much and what is going on this health information. So, the health information is generated by the disc, by the operating system and this is basically sent over the network if I want to send this information, the health information of the disc, I need to have control over the operating system, and I should also ensure that my network firewall does not stop its transmission, and it is possible only if I have control, I have controlled both on the operating system and also on the network. So, she went and looked at what is inside, what is the health, they found out that it is encrypted, but it was running to Mbs.

(Refer Slide Time: 15:49)



WISE GEN's Wisdom

- What is this information -
  - The manual tells "Health" and the information is encrypted
  - The disk vendor introduced by VVV alone knows the key to decrypt.
  - WISE GEN found the size of "Health" information to be too large and asked for clarification with VVV.
- On investigation she found that confidential information was sent in encrypted form to VVV for leak to competitors.
- Since all the infrastructure were maintained by VVV, it could create necessary rules in (network) firewall and also configure hardware accordingly so as to send such large packets carrying confidential information.
- The Gopalakrishna Committee (RBI) guidelines for IT infrastructure management in Banks advices different vendors for different components of the IT infrastructure.

The health of this may not be more than kilobytes, but it was running in megabytes. So, something fishy was going, other than the health of information something else also started moving out in the pretext of health, and people are when Wise Gen asked what is going on, they said it cannot be decrypted that encrypted key is somewhere else is etcetera. So, then after lot more of fight they found out what the key encryption is, then they found that some crucial directories are also zipped and send along with the health information.

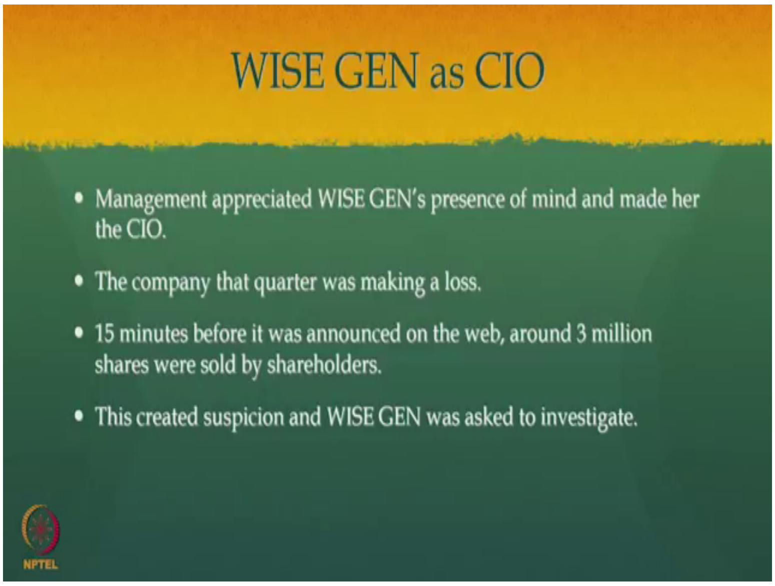
So, this all happens. So, the information started leaking through this part and this all happened, because the person who was handling the operating system and the person who was handling the networking are same. So, when I do a fraud that the operating system level, I can allow that fraud to percolate to the external world by making sufficient adjustment to the networking.

This could not have happened if A maintains the operating system and B maintains the networking, and in the interest of the company please keep them as isolated, then there is no way by which this large data could have passed the fireworks. So; the decision of the company, to give the A M C for all the major components like networking, database, hardware and operating system. All these things to a single vendor was the reason it was an; obviously, a correct logical reasoning, but still it, from a security point of view, it became a very bad decision.

So, if you look at a committee Gopala Krishna Committee constituted by RBI on the guidelines for how to build I T infrastructure in banks, there is very nice discussing on a, why different vendors should be in charged for different components. So, it is a must, though all that we have seen there was a failure, people were pointing fingers, does absolutely chaos and that is the reason why they put it on to the same fellow.

All these are logically coherent things, but from a security angle this indeed has led to a major a issues. So, based on this great thing, what Wise Gen found out, management appreciated Wise Gens presence of mind and made have the chief information officer, but because of these loss of tender, which she went and quote it very early, because of her intellect.

(Refer Slide Time: 18:10)



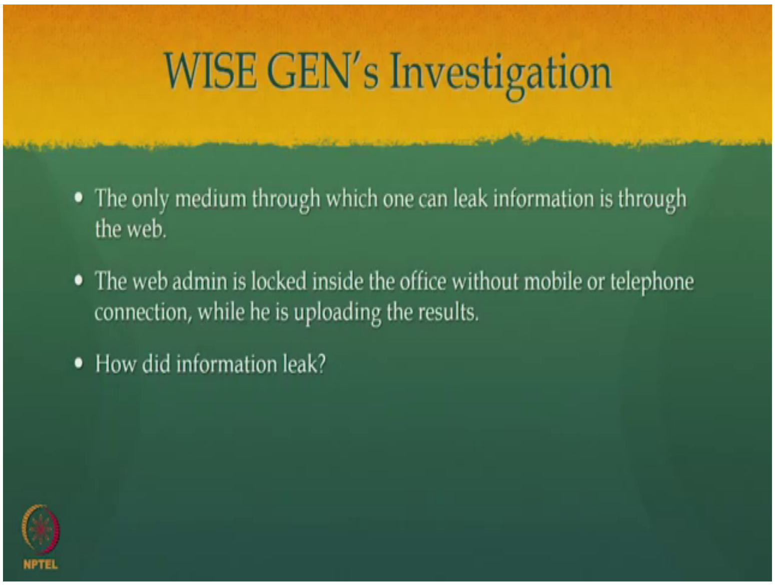
WISE GEN as CIO

- Management appreciated WISE GEN's presence of mind and made her the CIO.
- The company that quarter was making a loss.
- 15 minutes before it was announced on the web, around 3 million shares were sold by shareholders.
- This created suspicion and WISE GEN was asked to investigate.

The company that quarter was actually making a loss, but people externally did not know that they are making a loss now every quarter. So, this company have shares. So, every quarter if I hold a, if I am a publicly listed company, every quarter have at own results. So, before I announce the result and say I have a loss. If somebody else knows that I will have a loss, because if the moment I announced that I have a loss my share price will go down. So, if this information is got a little bit earlier that before I have announced the result that somebody comes to know that I am going to report a loss, then if they have my shares, they can immediately sell it. So, that they do not have occur a loss; that is why a publicly listed company, the directors of the publicly listed company are not allowed to trade in some window, where the results are going to be announced, this is called you know inside a trading and that should not happen right within some duration.

But what happened in this case again from when Wise Gen took over as C I O, she found that particular thing, because of the mismatch that happened that particular company was going to report certain loss, 15 minutes before the actual results were announced on the web, around 3 million shares were sold by shareholders. This created lot of suspicion and they asked Wise Gen to investigate how this information has leaked; obviously, somebody will not true you know, sell of 3 million shares. So; obviously, somebody should have known that there is a loss and how did this information leak.

(Refer Slide Time: 19:42)



WISE GEN's Investigation

- The only medium through which one can leak information is through the web.
- The web admin is locked inside the office without mobile or telephone connection, while he is uploading the results.
- How did information leak?

Now, let us look at the only medium through which one can leak information, is through the web, because when the results are being prepared, it has to be putdown the web. Only the web admin will know, because he is uploading the results and the directors are inside, no mobile phones are allowed. The web admin is logged inside the office without mobile or telephone connection while he is uploading the results.

So, nobody will know about it and show how this information leaked. Directors will not delete out, the only fellow who knows this the web admin and he does not have a mobile phone or telephone and then right. So, he just uploading the result, how will somebody know that. So, this is the question. Now; when I am uploading the result some 10 minutes before only he will also come to know, if because he is taking those things typing it and then uploading. He wants to make an HTML file and upload or is to give a link.

So, just 10 minutes before or 15 minutes before that real results is going to say go live, at that point only this web admin also will know. So, you will not know yesterday that will make a web page for it and then he will probably it. So, you only know the result 15 minutes and he has no access to phone, he has no access to internet, even this how will be how will be, how does this information leak. So, again I stop here in this section 3 and we will go out to session 4 to find out how did the information actually leak right. I hope you are enjoying this and we will see you in session number 4.

Thank you.