SWIFT is responsible

Head of govt probe body on $81m BB fund heist describes how SWIFT made the payment system vulnerable to cyber attack

A government committee probing the Bangladesh Bank heist has held SWIFT responsible for weakening the payment system which allowed cyber thieves to steal $81 million from the central bank's account with the New York Fed.

"Primarily, SWIFT is responsible for the incident," Mohammed Farashuddin, the head of the three-member panel, told reporters at the BB yesterday at his first media briefing on the heist.

Since the unknown hackers pulled off the history's biggest cyber heist on February 4, the Brussels-based SWIFT (Society for Worldwide Interbank Financial Telecommunication) has repeatedly maintained that its core message system with the BB was not compromised.

But Farashuddin said SWIFT linked its platform to the real-time gross settlement system or RTGS by removing antivirus software on its own system which left the entire network vulnerable to cyber attacks. Secondly, SWIFT did not put in place a hardware security module, a computing device that safeguards and manages digital keys for strong authentication and provides crypto-processing.

The system's initial design included a backup, but there has been no such backup in place as of yet, according to Farashuddin.

Last week, SWIFT rejected allegations by officials in Bangladesh that technicians with the global messaging system made the BB more vulnerable to hacking.

Farashuddin said, "SWIFT said all responsibilities rested upon Bangladesh. But it's not correct. It doesn't mean that we are rebuking SWIFT."

"But SWIFT must accept responsibility for the incident. They should help Bangladesh Bank."

SWIFT now says its job is to provide solutions and it's the client's responsibility to ensure the safety of the system, Farashuddin said. "I admit that."

But he emphasised that if SWIFT or any individual provides any system, it is the provider's responsibility to supply a secure system and make sure that it doesn't become vulnerable midway.

The SWIFT system has been working in Bangladesh since 1995.

In March last year, SWIFT wrote to the BB that the Belgian organisation wants to link the SWIFT platform with RTGS.

"The letter contained nothing but excitement and flattery. It didn't explain how Bangladesh and the BB would benefit if the linking goes ahead," said Farashuddin.

Upon receiving the letter, the bank's executive committee approved it in an irresponsible manner, and the decision was "devoid of common sense", he said.

Before the link was established, 13 steps should have been followed: some by SWIFT, some by the BB and some jointly by the two, he said.

But the SWIFT platform at the BB was connected with the RTGS in November last year without following two or three major procedures, he said.

The connection was supposed to be established after SWIFT provided the BB with a hardware security module. But SWIFT didn't do so.

Later, the module was brought in, but it is yet to be installed, said the former BB governor.

While establishing the link, it was found that the connection could not be established due to the anti-virus embedded with the SWIFT platform.

When the link was established, the SWIFT engineers tried to disable the anti-virus in vain. Later, the anti-virus was uninstalled because the two systems couldn't be connected while it was active, according to Farashuddin.

It appears that the BB officials involved in the matter were not aware of the changes, he said.

An engineer from SWIFT gave an interim connection, and it was agreed that once the regular connection was established, the interim connection would be removed.

But the interim connection was not discarded even after the regular connection was established, said the former BB governor.

The system's initial design included a backup, but no such backup has yet been put in place in the BB system, he said.

"But even after the establishment of the connection, SWIFT has not yet explained to BB officials how the system operates and what types of problems could surface."

The SWIFT engineers gave BB officials instructions to keep the server running round-the-clock – first verbally before their departure and later through telephone correspondences.

"Because of all these reasons, we think that SWIFT system had been compromised."

There was no logic behind establishing the connection between the SWIFT platform at the BB and the RTGS, he said.

The BB carries out international transactions through SWIFT while the RTGS processes local transactions. "There is no logic behind connecting local transactions with international transactions."

Farashuddin said 18 messages with payment instructions worth $500 million were sent from the BB back office to the Fed till 7:15pm on February 4.

Of the amount, $200 million was sent for buying bonds from Basel Bank.

Later that night, the hackers broke into the BB system and sent 70 payment instructions involving $950 million to the Fed.

"We haven't yet got evidence or proofs that BB officials have made those instructions."

The Fed outright rejected the payment instructions for 35 orders because intermediary banks were not at the recipients' ends.

Of the remaining 35, the Fed became suspicious and sought explanations from the BB about 12

payment instructions.

“But they should have known that it was already Friday in Bangladesh, and the Bangladesh Bank wouldn’t be able to give explanations,” said Farashuddin.

The Fed was suspicious about the 12 payment instructions and sought explanation from the BB, but didn’t get it. Still, the Fed carried out five payment orders.

“Why did they make payment? Why didn’t they issue the ‘stop payment’ order or recall the fund if they had felt it was suspicious?”

The Fed should have smelt a rat as it sent messages to the BB but didn’t receive any responses, he said.

Of the five payment orders, the beneficiaries of the four were individuals. Historically, BB’s payment instructions involving large amount are institutional. In case of individuals, the amount is small, said Farashuddin.

Farashuddin the hackers had made attempts to steal $950 million. Of them, advices worth $101 million were sent.

BB got back $20 million because of misspelling of the beneficiary organisation in Sri Lanka. Now, the amount of the missing money stood at $81.16 million.

He said the malware was created either in Pakistan or North Korea.

“We have got evidence that this malware was created to hack the BB’s reserves.”

Talking about the responsibility of the BB, he said the decision to establish connection between the SWIFT platform and the RTGS was inconsiderate.

“It should not have been done.”

BB’s officials were unskilled, negligent and careless about the issue, he said.

“We have no doubt about it. However, we have not received proof yet that they were part of the theft. We are trying to find it out.”

The Farashuddin-led probe body has tasked three professors from Bangladesh University of Engineering and Technology (Buet) to find out whether anybody from the BB was involved with the scam.

Yesterday, the three-member team submitted an interim report to the probe committee.

The probe body is collecting information about two BB officials, said Farashuddin.

“However, the information we have received so far indicate that they were not a party to the crime.”

About the recovery of the stolen funds, he said the government and other departments concerned would work jointly to retrieve the money.

Quoting the Filipino-based Inquirer media outlet, which broke the news, Farashuddin said Philippine’s casino junket operator Kim Wong is believed to have been holding $35 million and remittance company Philrem $17 million.

“It is possible to recover more than $50 million.”

He said diplomatic strategies and legal tools have to be used to recover the stolen money, he said.

“We have to take assistance from the Fed. We have learnt that they are ready to help.”

Last week, the Fed, the BB and SWIFT vowed to work together to trace the stolen $81 million, following their first-ever joint meeting in Basel, Switzerland.

Farashuddin said Bangladesh should try to convince the Fed to put pressure on the three US-based intermediary banks that channelled the $81 to the Philippines.

The Fed could also pressurise Rizal Commercial Banking Corporation as it has a branch in Los Angeles.

“If we file lawsuits and work jointly, we will perhaps be able to recover the majority of the missing money.”

He said it was not right on the part of the BB to have kept the government in the dark about the theft.