**Hacked: How $171 mn stolen from Union Bank was recovered Details emerge of how the money was retrieved from accounts in four different countries after government intervention**

**Even as the government marked Digital India Day, encouraging more Indians to move to banking online, investigators and cyber security agencies are battling more breaches of banking transfer security, admitting that “non-state” actors are increasingly targeting India.**

**Details are only just emerging of the biggest such hack of $171 million in July 2016, which necessitated a seven-country hunt that had to be spearheaded at the top levels of government to reverse the theft. The hack involved a transfer double the size of the Bangladesh Central Bank that lost $81 million in February 2016, but most details have been kept under wraps so far.**

**Chairman of the Union Bank of India Arun Tiwari as well as India’s cyber security chief, Dr. Gulshan Rai, who were involved in the operation, confirmed to The Hindu that while the attack was serious, all of the money had been retrieved within days.**

**“We worked in record time with the Reserve Bank of India, bank authorities and government agencies coordinating efforts. The bank succeeded in blocking the transfer of funds and credited the entire amount in a record period of six days,” Mr. Rai, who is the country’s first Chief Information Security Officer, said.**

**“Investigations have been carried out by different agencies. And whatever was suggested [to improve security], has been implemented,” Mr. Tiwari said.**

**Events unfolded on the evening of July 20, towards the end of the bank-week, officials said, piecing together the sequence. On that Thursday, a Union Bank of India official in the treasury department looking at SWIFT (Society for Worldwide Interbank Financial Telecommunication) payments was checking statements for the day from their dollar account, when he noticed a startling discrepancy. An amount of $171 million had been debited from the bank without his authorisation. He quickly raised a red flag to the bank’s top management about the transaction. “I haven’t authorised any such payment last night,” he reportedly told the bank’s management.**

**By then the money had found its way to at least five locations, including accounts in Cambodia’s Canadia Bank and RHB IndoChina Bank, Thailand’s Siam Commercial Bank, Bank Sinopac in Taiwan, and a bank in Australia. These funds were routed by Citibank New York and JP Morgan Chase New York, which hold UBI’s foreign exchange accounts.**

**MEA steps in**

**According to cybersleuths, who were brought into the investigation, the hacking had occurred by sending malware to a bank official, who mistakenly opened an email that enabled the robbery. By the next day, when the extent of the loss was known, senior officials of the Ministry of External Affairs and other offices in South Block were pressed into action to retrieve the money.**

**One tricky negotiation was with the Taiwanese government with which India doesn’t have diplomatic ties, particularly as a court order was needed to secure the banking reversal instruction. However, with some pushing from U.S. officials, the entire $171 million was traced.**

**As the money trickled back into their accounts, Union Bank officials heaved a sigh of relief. Despite the speed and efficiency of operations to recover the money, not much is known about the follow-up investigations. An FIR was filed only a month later on August 25 (FIR 243/2016) at Mumbai’s Cybercell, but bank officials said they had no information of further follow-ups including details of a charge sheet, or investigations in any of the six other countries involved.**

**(With inputs from**

**Vijaita Singh)**