SWIFT AND THE BANGLADESHI BANK HEIST

I've been following the story of how what are described to be criminal hackers tried to steal $1 billion from Bangladesh's national bank, in part because of the tie to SWIFT, the financial transfer company (as of now, $81 million are still missing, but Sri Lanka and the Fed managed to reverse or prevent the remainder of the theft attempt). As part of the hack, the thieves stole Bangladesh's SWIFT credentials (it appears they did this after Bangladesh connected the server running SWIFT transactions to 3 other servers).

> "Malware was specifically designed for a targeted attack on Bangladesh Bank to operate on SWIFT Alliance Access servers," the interim report said. Those servers are operated by the bank but run the SWIFT interface, and the report makes it clear the breach stretches into other parts of the bank's network as well. "The security breach of the SWIFT environment is part of a much larger breach that is currently under investigation."
>
> SWIFT is a member-owned cooperative that provides international codes to facilitate payments between banks globally. It can't comment on the investigation, according to Charlie Booth from Brunswick Group, a corporate advisory firm that represents SWIFT.
>
> "We reiterate that the SWIFT network itself was not breached," Booth said in an e-mail. "There is a full investigation underway, on what appears to be a specific and targeted attack on the victim's local systems." SWIFT said last week its "core messaging services were not impacted by the issue and

> continued to work as normal."
>
> Dedicated servers running the SWIFT system are located in the back office of the Accounts and Budgeting Department of Bangladesh Bank. They are connected with three terminals for payment communications.

While SWIFT insists it has not been breached, the hackers used a name making it clear they were targeting the SWIFT system.

> On Jan. 29, attackers installed "SysMon in SWIFTLIVE" in what was interpreted as reconnaissance activity, and appeared to operate exclusively with "local administrator accounts."

SWIFT is sending out a security advisors to its members, advising them to shore up their local operating environments.

> On Jan. 29, attackers installed "SysMon in SWIFTLIVE" in what was interpreted as reconnaissance activity, and appeared to operate exclusively with "local administrator accounts."

In separate news, a local security researcher who had been working on the hack disappeared last week.

> In a weird turn of events, one of the security researchers who voiced their criticism at the central bank's security measures disappeared on Wednesday night.
>
> Family members are saying that Zoha met with a friend at 11:30 PM on Wednesday night, March 16. While coming home, a jeep pulled in front of their auto-rickshaw, and men separated the two, putting them in two different cars.
>
> Zoha's friend was dumped somewhere in the city (Dhaka) and was able to get

> home by 02:00 AM, the next day. He then contacted Zoha's family, who said the security researcher never came home.
>
> The next day, family members tried to report the researcher missing, but police officers just kept redirecting them from one police station to another until the family gave up and contacted the media for help.
>
> [snip]
>
> According to BDNews24, Zoha was a former collaborator of Bangladesh's ICT (Information and Communication Technology) Division and worked with various government agencies in the past. It appears that his comments about the Bangladesh central bank cyber-heist were made working as a "shadow investigator" for a security company that family members declined to name.
>
> Answering questions about his own investigation into the central bank's cyber-heist, Zoha said that the "database administrator of the [Bangladesh Bank] server cannot avoid responsibility for such hacking" and that he "noticed apathy about the [server's] security system."

From this description and those based on the FireEye report, it seems like Bangladeshi authorities, and not SWIFT, would be the powerful people who might want to make this guy disappear. But I find it interesting that someone who was presumably mirroring FireEye's work has apparently been kidnapped.

Remember: NSA's TAO hackers hacked into SWIFT (even though the US has access to SWIFT to obtain counterterrorism information via an intelligence agreement anyway), apparently by accessing printer traffic from what sounds like member banks.

> The NSA's Tracfin data bank also contained data from the Brussels-based Society for Worldwide Interbank Financial Telecommunication (SWIFT), a network used by thousands of banks to send transaction information securely. SWIFT was named as a "target," according to the documents, which also show that the NSA spied on the organization on several levels, involving, among others, the agency's "tailored access operations" division. One of the ways the agency accessed the data included reading "SWIFT printer traffic from numerous banks," the documents show.

While we don't have enough detail to assess, it does sound like the NSA got in through vulnerabilities at the member bank level, like these thieves did.

Again, I assume the kidnapping is best explained by Bangladeshi efforts to cover up their own incompetence. But I do find the possibility that SWIFT might be vulnerable due to vulnerabilities at its member banks, too.