DIGITAL HEIST

Who guards the guardhouse?

ZIAUDDIN CHOUDHURY

IN a surreal digital theft that befits a high octane movie thriller, we were recently informed of the daring heist at Bangladesh Bank in which nearly a billion dollars were siphoned off last month. As if this was not enough, the theft took place over several days early February through a series of about three dozen electronic fund transfers from the Bank to New York Federal Reserve for a total amount anywhere between eight hundred fifty to eight hundred seventy million dollars. All of the looted amount made through dozens of transfers would have been cashed had it not been due to the now famous spelling error in a twenty million check made to a Sri Lankan NGO. The error prompted the routing bank, Deutsche Bank, to seek clarification from the Bangladesh central bank, which stopped the transaction. But the mystery hackers still managed to swipe $80 million, one of the largest recorded bank thefts in history.

The news struck the headlines in the foreign press, particularly in the UK and the US, but what was possibly more puzzling to everyone is how a spelling error stopped a bank heist than the actual massive pilferage of funds from a central bank. The news highlighted the ability of a spelling error to stop the attempted digital robbery. It is through further investigation that news agencies came to know of the successful transfer of at least $80 million to the Philippines. All major news agencies referred to this latest heist as another instance of CEO fraud, a growing threat to world financial institutions that had cost globally $2 billion in the last two years.

So what is actually a CEO fraud, and how does the attack work? The scam is referred to as a CEO fraud because the perpetrator or perpetrators pose electronically as the chief executive or senior financial official of an institution they are targeting. For an attacker to successfully pull it off, they need to know a lot of information about the company they're targeting. Much of this information is about the hierarchical structure of the company or institution they're targeting. They'll need to know who they'll be impersonating. Although this type of scam is known as "CEO fraud", in reality it targets anyone with a senior role – anyone who would be able to initiate payments. They will need to know their names, and their email addresses. It would also help to know their schedule, and when they will be travelling, or will be on vacation. Experts say the criminals managed to breach Bangladesh Bank systems and stole the credentials of its senior officials for online payment transfers. (The Federal Reserve of New York stated that the transfers had valid digital credentials of Bangladesh Bank.)

Frauds and scams that target corporations and financial institutions have happened before, but probably it is the first time a central bank was successfully targeted. The most sobering aspect of the heist is the divine intervention in foiling of the robbery in its entirety in the form of a spelling error. It saved the bank much of the heist amount, and it could possibly recover some of the eighty million dollars that got away. It is also possible that with the help of international cyber security experts, that the bank has engaged, the source of the breach can be identified as well as corrections made in the bank's system to prevent future breaches.

But the most unsettling part is the apparent revelation to the government by the bank's news of the breach and heist after a month of its occurrence. There may be defense of some kind or the other for this delay, but it will be ludicrous to assume that the bank authorities chose to go hush-hush, lest the news adversely affects the financial market. A serious crime of this magnitude is not a paltry incident of burglary in a government office that may not warrant waking up the minister at night and reporting it to him. It is a major incident of financial loss just not to the bank, but the country of which the bank is a financial guard. Keeping news hidden from the government is like a house guard concealing the news of theft in the house from his master.

The original hacking of Bangladesh Bank happened between February 4 and 5, 2016, when the bank's offices were shut. Security experts said the perpetrators had deep knowledge of the Bangladeshi institution's internal workings, likely gained by spying on bank workers. This is not to say that some bank employees could be complicit, because the CEO fraud, as said earlier, does not necessarily require direct assistance of employees of the institution. They only need to follow the workers closely.

Perhaps in time, we will come to the bottom of this heist and find ways to prevent such occurrences in the future. But these will concern computer systems and digital security apparatus. What these will not do is change the human guards who watch over the institutions and their behaviour and determine how to react responsibly in crisis situations and own up to mistakes. This requires training and change of management of a different kind; one of accountability and leadership and courage to take responsibility for mistakes.

The writer is a political analyst and commentator.

Frauds and scams that target corporations and financial institutions have happened before, but probably it is the first time a central bank was successfully targeted.

Right to Information: Impact of High Court ruling

SHAMSUL BARI *and* RUHI NAZ

AN important development took place last month regarding the Right to Information (RTI), which is likely to have significant impact on the transparency regime. It concerned a ruling by the High Court Division (HCD) on a decision of the Bangladesh Information Commission (BIC).

The ruling resulted from a writ petition filed by six Bangladeshi citizens who were aggrieved by a decision of BIC on a complaint submitted to it earlier under the RTI Act. The court had two questions before it: one, whether citizens had unfettered access to information held by the Election Commission (EC) on audited annual statements of income and expenditure submitted to it by political parties; and two, whether the desired information was "third party" information which required checking if the parties considered it "secret information" under Section 9(8) of the RTI Act. The petitioners had submitted that the information concerned was public information and thus, required no "third party" clearance. BIC took the opposite view.

After preliminary hearing, HCD issued a Rule Nisi, calling upon BIC to show cause why the said decision should not be declared to have been passed without lawful authority and of no legal effect. The ruling was made absolute on February 18, 2016, which meant the Court found in favour of the petitioners.

Section 9(8) of the RTI Act requires a Designated (Information) Officer of a public authority, dealing with a request for information, to check if the said information "has been supplied by a third party or a third party's interest is involved in it and the third party has considered it as secret information." If so,the DO is required to seek the opinion of the "third party" before acting upon it.

Let us now relate the law to the facts of the case. The six petitioners of the writ are various office-bearers of Shushashoner Jonno Nagorik (SHUJAN), a Bangladeshi NGO which seeks to promote democracy and good governance in the country. A number of them had submitted an RTI application in June 2013 to the Designated Officer (DO) of the EC requesting photocopies of all available audited annual statements of accounts filed by registered political parties with the EC over the years.

In his response, the DO informed the applicants that the information sought were not EC's own information, and should be collected directly from the political parties. Unhappy with this, the applicants preferred an appeal, under Section 24 of the RTI Act, to the Appellate Authority of the EC, which affirmed the decision of the DO.

The applicants then filed a complaint to the BIC under Section 25 of the RTI Act. At its hearing on October 22, 2013, the BIC agreed with the EC position that opinion of the "third-party" was indeed necessary, and asked the applicants to reapply to the EC, specifying names of political parties and the time period for which information was sought. The EC in turn was directed to write to the concerned political parties, seeking their opinion on the request.

Following this and after further back and forth, the applicants were informed by the EC that out of 21 registered political parties, only three, namely Bangladesh Muslim League, Jatiya Somajtantrik Dal (JSD) and Bikalpadhara Bangladesh, had consented to the disclosure of the requested information. The EC was willing to act accordingly.

Being dissatisfied with this response, the applicants submitted a review petition to the BIC stating that its earlier decision laying down a requirement of seeking consent from "third-parties" was incorrect, as the information sought were "public information", which every citizen was entitled to access from the EC under Section 4 of the RTI Act.

BIC responded by saying that as there was no scope for review under the RTI Act, a fresh complaint was necessary. This was submitted, whereby BIC reaffirmed its earlier decision. With all RTI avenues thus exhausted, the complainants filed the writ petition.

RTI enthusiasts, activists and scholars will now have to await the reasons for the court ruling. These will help all concerned, including the BIC, to deal with this and other provisions of the Act that pose problems for interpretations. It may, however, be said in anticipation that a contextual reading of the law by the learned commissioners could perhaps have avoided the need for the writ petition. For, it may be argued that Section 9(8) seeks to safeguard "third party" information only as circumscribed by the objectives of the Act.

It may be noted that secrecy was neither requested by the political parties in their submissions to the EC nor could they have done so. This is because they are required to provide the information under Political Parties Registration Rules, 2008, framed under Article 94 of the Representation of the People Order, 1972. This is patently public information. A positive approach to the application of the law on the part of the EC and the BIC would have shown that the question of secrecy did not arise at all. Moreover, no other provision of the Act had prevented the EC from disclosure of the information.

Two concluding remarks may be pertinent here. The first relates to interpretation of the law. Among many principles of interpretation, one is *noscitur a sociis*, which in English means "a word is known by the company it keeps". Applying that principle, the word "secret" in Section 9(8) of the RTI Act, read in conjunction withother provisions and intent of the Act, which is to replace secretive governance with transparency and accountability, would call for qualified application. It is useful to recall that there is a growing international practice which favours disclosure over secrecy wherever public interest clearly overrides other interests.

The second remark relates to the status ofpolitical parties under the RTI Act. Do they not qualify as "public authority"? Shouldn't citizens be able to obtain the information on income and expenditure, or any other information on their work, directly from the political parties, without going via the EC? In our view, the answer to both should be "yes". However, they have not arisen in a RTI case in Bangladesh yet. In India, they have and the result was electrifying.

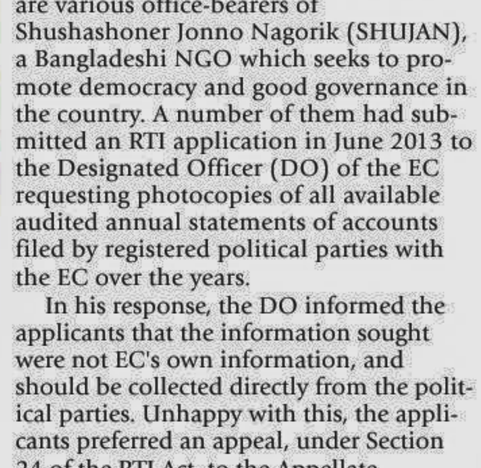
In the Indian case, two years ago, the Central Information Commission (CIC) ruled that political parties do indeed qualify as "public authority". They based their decision on a liberal interpretation of Section 2(h) of the Indian RTI Act 2005 which includes as public authority any "non-government organisation substantially financed directly or indirectly by funds provided by the appropriate Government". In doing so, they considered submissions describing various support/facilities Indian political parties received, directly or indirectly, from the government. The ruling was challenged in the High Court by the political parties, where it remains pending. [See also our column of August 16, 2015 in this newspaper.] The Bangladesh RTI Act 2009, in Section 2(b) includes as public authority: "any private organisation or institution run by government financing or with aid in grant from the government fund". Would BIC find our political parties to qualify as "public authority" under this section, given the various facilities/concessions they receive from the government? We will have to wait for an RTI application to put the matter to test.

The writers are Chairman, Research Initiatives, Bangladesh (RIB) and Project Coordinator (RTI section) of RIB respectively. Email: rib@citech-bd.com.

CROSSWORD BY THOMAS JOSEPH

ACROSS
1 Muffles
6 Croc's cousin
11 Chicago airport
12 Animated
13 Women's quarters
14 Specified
15 Blood bearer
17 Role for Craig
18 Castor, for one
20 Spoken
22 Finish first
23 Speedy horse
26 Heart, e.g.
28 Molten rock
29 Poseidon and Neptune
31 Band blaster
32 Gambling center
33 Debate group
34 Seed holders
36 Niger neighbor
38 Notions
40 Believed without question
43 Angola neighbor
44 Washer cycle
45 Hot crime
46 Tough puzzle

DOWN
1 Cry from Homer
2 Cry of insight
3 Yellow Monopoly property
4 Hog the mirror
5 Convoy truck
6 Comic bit
7 Thieves' outwitter
8 Copenhagen park
9 Kitchen sight
10 Tear
16 And not
18 Noah count?
19 Marionette over
21 St. Louis team
23 Shortly, in poems
24 Clip contents
25 Snoozes
27 Way back when
30 Clinic nickname
33 Barbecue spot
34 Layout unit
35 Sneaker problem
37 Angel's instrument
39 Junior
41Try out
42 For every



3-11

YESTERDAY'S ANSWER

P	A	C	E		A	M	P	S	U	P
I	R	O	N		M	O	L	I	N	E
T	E	N	T		I	N	A	R	O	W
S	A	C	R	I	S	T	Y			
		E	A	T		H	A	C	K	S
S	W	A	P	S		S	T	O	N	E
P	A	L						N	E	W
A	V	E	R	T		R	A	G	E	S
R	Y	D	E	R		O	R	E		
			T	I	T	I	C	A	C	A
M	O	J	A	V	E		A	L	A	N
A	W	A	K	E	N		R	E	N	T
T	E	N	E	T	S		O	D	E	S