Questions about BB fund heist

PRABEER SARKAR

AN obvious case of a targeted attack, using vulnerability exploit tactics, the 100 million dollar Bangladesh Bank heist will remain one of the most profiled cyber crime case studies throughout 2016. It has all the ingredients of a bestseller. A star victim, none less than the central bank of a country, a sizeable value of crime in terms of money, and a media coverage following the story of how the money moved across countries and banks and casinos and chips -- a classic cyber crime thriller material.

However, the incident is real. The hacking has happened. Our central bank reserves have been robbed of millions. Whether we can recover the amount (as Bangladesh bank officials are claiming) or not, the fact remains that our central bank is vulnerable. It also means the entire financial and banking sector of Bangladesh is vulnerable.

These could have been remote hack exploiting vulnerabilities in the system, or an intrusion based hack in collaboration with insiders (which some are trying to call a malware attack) or even a state or organisation sponsored attack. The "sponsored" attack part may seem like a conspiracy theory, but only to be written off after a full professional and certified cyber intelligence investigation. I repeat the word investigation, which is not to be mixed up with the concept of incidence response management. Unless we have a professional level investigation the facts of the incidence and the vulnerability loops and identification of involvements will never be discovered. From what is coming out in the media it seems that the central bank focus is on incidence response. It is a step towards speculated cure but not diagnosis and a way to future preventions.

The hacking of the Bangladesh Bank system is not a real life bank robbery. The crime scene is not at the bank premises. It is on cyber space -- on computer servers across the globe, in devices the hackers have used, across the internet traffic used in the operation starting from the Bangladesh Bank servers, in logs and files and activity of the systems linked.

The hackers are talented and they would have masked their paths. It is important to first investigate, come to a finding and then start planning and implementing a security system for the infrastructure with proper solutions and practices in place. Without a diagnosis there will be no prescription.

Nevertheless, the Bangladesh Bank incidence is just the tip of an iceberg. Not a caution beep but a mega horn. The cyber threats everyone loves to talk about in seminars and symposiums are now real right on our tables. And it is ugly. The concern is not just about the incidence at hand, but at what it has brought out to light.

1. Our central bank does not have a chief security officer in IT. Is there anyone and a team responsible for cyber security? Cyber threats and security are standard issues. It cannot be that the central bank does not have responsible and dedicated personnel for cyber security. If there is, question is why the CSO is not answering the questions to the queries or why the personnel commenting and answering are not identifying themselves as cyber security personnel. Again what are the opinions of the central bank's IT team and findings on the incidence?

2. Media reports suggest that the corresponding Bangladesh Bank servers are not firewall protected. That again cannot be. It is a standard procedure particularly in a crucial infrastructure. What are the access policies? Who controls the policies? How are the policies implemented? What measures were taken to filter web based attacks? Who is answerable to the questions related to this?

3. The central bank's IT head (or maybe joint heads) has not identified himself or themselves and accounted for the incidence.

4. Clearly enough the central bank is not prepared for an incidence like this. No reason why they should not have been. The nation is moving through a digital revolution. The central bank itself has comments and statements on digital developments of the Bangladesh banking sector. They must have been going through various cyber security reports and alerts. Did they not subscribe to professional cyber threat intelligence services and reports? This is the central bank of a country. This is all standard in the IT world. Seems they had no plan or policy on reporting or responding to a cyber incidence at all. Answering to the press has been a PR failure also as nothing has been clearly stated or denied even.

5. Neither the central bank nor the government has an emergency response policy, plan or team for cyber incidences. Nor do they have a plan to contact the right agencies and establishments in a crisis situation like this. No authorised contracts. No advance threat intelligence service subscriptions. No specific point to consult with. It's all being done now in the midst of a commotion in bits and patches. How are the security experts involved at the moment being vetted? Are we giving access to any form of investigation on a central bank transaction system? What about national security?

6. Does the central bank have regular certified cyber security related trainings for dedicated team members? If they have, what are that team's findings and opinions? Security training is a standard process in a mission critical IT setup.

7. There are stories about involving the US Secret Service and FBI in the investigation process. As far as it is concerned it should be the Interpol's cyber intelligence team. The crime has been carried out across the borders beyond the US and Bangladesh. The Interpol carries out investigations in collaboration with all the countries across borders.

8. Imparting speculative comments on the incidence before a concluded investigation harms the image of the country and hampers the investigation process. The concerned and the media should take that into serious consideration. Everyone seems to be having a say on the incidence without responsibility.

Questions and observations can continue. But the base line is that we were not ready for a cyber threat. We are not ready even now. If the central bank is not secure, the other banks in Bangladesh are not also. That brings to questions on our national power grid systems, crucial government infrastructures or even the national ID database. How secure are we? What security measures are maintained? Why don't we have a national IT chief security officer with an expert and trained team at disposal?

The time is past already. The incident of hacking has been an expensive eye opener for us and our lacking is great news for the cyber criminal community. We can expect more threats now. And this is just one area. We haven't spoken yet about our children being bullied online, our women being harassed on the net, random access to pornographic contents having serious impact on the social aspects, or terrorist targeting propaganda across the circuit. Establishing a cyber security platform is not a one day run. It takes a long time covering various aspects. And there is no magic formula for an instant cure.

We live in a connected world and will remain to live so. And in this world, cyber threats are real. It's time to take the right steps and implement the right solutions and practices in cyber security.

The writer is CEO of Officextracts.

STAR/FILE

The incident of hacking into a Bangladesh Bank account with the Federal Reserve Bank of New York has been an expensive eye opener for the country.

GM, Ford announce investments in driving technology

BBC NEWS

US carmakers General Motors and Ford have both announced strategies geared at taking on the tech world's growing influence in the car industry.

GM will buy Cruise Automation, a firm that creates self-driving technology.

Ford will set up a Silicon Valley-based subsidiary to invest in car-sharing and ride-hailing services.

Both have been making investments in technology to boost their role in the personal mobility market, that is moving away from driving.

GM has not disclosed how much it will pay for Cruise Automation, in a deal expected to be completed in the second quarter of 2016.

The company has been testing its self-driving cars in San Francisco and should help GM in its quest to beat Google to be the first producer of consumer-ready self-driving cars.

Cruise Automation will operate as an independent unit within GM's automated driving division.

"Fully autonomous vehicles can bring our customers enormous benefits in terms of greater convenience, lower cost and improved safety for their daily mobility needs," said GM president Dan Ammann.

Ford has been testing autonomous vehicles and ride-hailing services in London and Kansas City.

The new subsidiary - Ford Smart Mobility - will invest in these sectors further. In a statement, the company said: "Ford is aggressively pursuing emerging opportunities."

The unit will not initially be reported in Ford's earnings statements.

"Our plan is to quickly become part of the growing transportation services market, which already accounts for $5.4 trillion in annual revenue," said Ford's chief executive Mark Fields.

Ford Smart Mobility will be run by Jim Hackett, the former head of office furniture and technology supplier Steelcase.

India bans over 300 combination medicines

REUTERS, *New Delhi*

India has banned the manufacture and sale of more than 300 combination medicines sold without approval from the central government, a senior health ministry official said on Saturday.

Fixed dose combinations are used worldwide to improve patients' compliance, as it is easier to get them to take one drug rather than several. But inconsistent enforcement of drug laws in India has led to the proliferation of hundreds of such combination medicines entering the market based on approval from regulators of individual states.

Nearly half the drugs sold in India in 2014 were combination medicines.

"Now based on responses (and) assessment of products, more than 300 drugs have been prohibited," KL Sharma, a joint secretary at the health ministry, told Reuters.

REUTERS/FILE

A medical representative, *centre*, talks to a chemist at a market in Pune, India.

US to send attachés to foreign markets to boost digital trade

REUTERS, *Washington*

The US Commerce Department said on Friday it would begin deploying digital trade experts in overseas markets as part of a pilot program intended to help US businesses navigate foreign Internet regulations when selling digital products or transferring data abroad.

The digital attachés will rely on "on-the-ground expertise" to provide export assistance to firms trying to understand and comply with another country's Internet policies, such as data localization requirements, US Commerce Secretary Penny Pritzker told Reuters in an interview.

"This is a new area that needs more specialised attention," Pritzker said.

The pilot program is launching in six to eight markets, including Brazil, China, Japan, India, the European Union and the 10-member Association of Southeast Asian Nations, or Asean, a Commerce Department spokeswoman said. Each market will have one attaché.

The United States exported about $400 billion in digitally deliverable services in 2014, according to the Commerce Department.

The attachés are modeled after the department's foreign commercial service officers who already work to promote trade across other sectors of the economy, such as agriculture and pharmaceuticals, Pritzker said.

"We'll have someone in that country, someone who will understand the specifics of how to sell your digital product," she said.

The move comes as the United States and European Union are working to implement the so-called Privacy Shield legal framework that will allow companies to easily transfer personal data across the Atlantic. The previous agreement, known as Safe Harbor, was struck down last year by the European Court of Justice following revelations about US surveillance programs.

China's labour law under fire as restructuring threatens jobs

REUTERS, *beijing*

China's labour protections are coming under fire from high places as economic restructuring pits officials concerned about social stability against a lobby arguing inflexible policies are stifling job creation and suppressing wages.

Company executives, especially at foreign or private firms, have long been critical of labour contract legislation and minimum wage laws that make it difficult for owners of an ailing business to turn it around or find willing buyers.

Now policymakers anxious to modernise China's slowing economy and slash overcapacity in heavy industry are making similar noises.

The export powerhouse province of Guangdong, a trillion-dollar economy that often leads the way on market reforms, said on Tuesday it would scrap scheduled rises to the local minimum wage in 2016, and keep it at 2015 levels - slightly over 1,500 yuan ($230) per month - through 2018.

On the same day, the official Xinhua media service highlighted comments by finance minister Lou Jiwei, who criticised China's Labour Contract Law in a speech during the annual meeting of parliament.

The law dates to 2008, when China had a reputation for sweatshops staffed by underpaid workers, an embarrassment for a ruling party that monopolised power in the name of socialism.

The law fixed a 40-hour working week for most employees, regulated maternity leave, and required businesses to be able to prove their case for sacking employees for incompetence or criminality or face heavy penalties.

Its standards aspire to those of developed economies, rather than emerging markets, though enforcement is weak. The EU, for example, limits the working week to 48 hours, while China's maximum is about the same, after allowing up to 36 hours a month overtime.

Regulations say minimum wages should be between 40 and 60 percent of the local average - though in practice 30-40 percent is typical - compared with about 30 percent in the United States and 50 percent in Britain.

Protections against dismissal are comparable to Japan's.

"The Chinese government wanted the best, the most polished labour legislation they could find, and simply imposed it on an economy that couldn't cope with it," said Geoffrey Crothall, communications director at China Labour Bulletin.

Chinese wages have risen at double-digit rates since the 2008 act, so factory workers now earn significantly higher than competitors in Bangladesh, Vietnam and Cambodia, and some think labour protections are hampering an economic transformation that will benefit workers in the long run.

"For enterprises and employees, the extent of protection afforded by the Labor Contract Law is unbalanced," Lou said, adding it encouraged companies to moves jobs from China to other countries.

"Who eventually bears the costs? The working class who the law was intended to protect," Lou said.

Labour activists say the protections are still needed, and businesses often break labour law with impunity, especially if they have local government connections.

The Xinhua article was circulated in both Chinese and English with supportive comments from regulators, exciting speculation that changes to the law could be afoot.

The timing could suit Beijing, which aims to reduce overcapacity in several industries, laying off an estimated 6 million workers at state-owned firms in the process.

It wants to do so without a spike in unemployment or crimping domestic consumption, but strong labour protections make companies unwilling to create new jobs or pay much for the jobs they do create.

Danny Lau, who owns a factory in Dongguan city in Guangdong, said he expected the government would soon "consolidate and streamline" the contract law to lower costs for manufacturers.

That would be welcome news to businesses exasperated by official interference in their operations.

"We have these government bureaucrats who show up at our facility arbitrarily, and they say, 'Let's look at your payroll'," said Ravin Gandhi, CEO of GMM Nonstick Coatings, which runs an office in Dongguan.

"And they say, 'Thirty percent of your facility workforce is going to get a pay raise. These people here are going to get 15 percent.' They don't look at your profitability, nothing."

As a result, GMM opened its next facility in India, which Gandhi said was 40 percent cheaper than China, even allowing for inferior infrastructure.

"Of course I'm going to take my foot off the gas pedal (in China)," he said. "I'll put those dollars in India."

When Reuters visited a printing factory in Chongqing in January, the boss was interrupted mid-interview by local officials, who had come to make sure he had paid salaries before the Lunar New Year holidays.

"(Last year) they called us into a meeting and said, 'You can't lay off employees'," he added.

Many economists say China has posted lacklustre business activity and investment figures - while official unemployment stays below 5 percent - precisely because companies saddled with high wage bills and low profit margins can't cut debt or invest.

"It's better to support workers than supporting loss-making firms," Li Yining, an economist at Peking University, said on the sidelines of the annual parliament meeting on Sunday.

REUTERS/FILE

Workers shout slogans as they protest at an IBM factory in Shenzhen, China.