Cybercrime As A Possible Cause For The Next Financial Crisis

You are in the line to pay for your takeout lunch and your card gets rejected, surprised you try again (since it worked perfectly well when you paid for coffee in the morning), worried you check the banking application on your smartphone to realise your account balance is zero, on enquiring with the bank you realise that you are a victim of a cybercrime (fraud); Imagine what happened to your personal bank account happens to all customers of a bank, or maybe a central bank of a nation, sounds unlikely? Think again.

In February 2016, hackers got away with one of the biggest thefts in history, robbing Bangladesh's central bank of more than $81m. Within minutes millions of dollars were stolen from Bangladesh's central bank via the Federal Reserve Bank of New York, transferred to accounts in the Philippines and then off-shored via Philippine’s casino system. How? The hackers entered into the Bangladesh Bank by sending phishing emails to employees of the bank and by gaining access to the bank’s network allowing them to send messages via SWIFT. SWIFT is the Society for Worldwide Interbank Financial Telecommunication and is a consortium that operates on a closed trusted computer network for communication between member banks around the world which process about 25 million money transfers daily. The attack had a potential to cause even more damage and only a typo prevented a $1 billion that was targeted. The alarming fact is most banks in the world are using the very network that was compromised. This is one of the many cyber-attacks on financial companies with varying degrees of success around the world.

The 2018 Global Risks Report identified cyber-attacks as a top-5 risk to doing business in 23 of the 35 OECD member countries and as the most significant risk in 11 member countries. The annual economic cost of cyber-crimes is now estimated to be over USD 1 trillion, far more than the record $300 billion of damage due to natural disasters in 2017. Hence, cybercrime be the cause of the next financial crisis due to the following reasons:

Correlation of Risks

In an hypothetical scenario: A criminal gang or a rogue state hack into a central bank, a custodial bank or a clearing firm that settles daily stock, bond and derivative trades. There are not many of these firms, so they are 'systemically important.' Say this hack disrupts the operations of one or more of these firms to the point that their services shut down and key data is damaged or destroyed, leading to a systemic risk. A risk which multiplies in magnitude to a positive correlation between the risks i.e. the effects ripple across other financial services firms to disastrous effects, and the entire global financial system could be bought to its knees. A large-scale cyber-attack could disrupt the operations of more than one financial companies and spread through the financial networks to the entire system, threatening financial stability in the economy at large.

The correlated nature of the financial sector, with inter dependencies between the central banks, the federal banks, IMF, world bank, various stock markets, government revenue

collection agencies, SWIFT and other international networks has led to the Harvard business review among many others have ranked cyber-attacks as the biggest threat facing the business world today, ahead of terrorism, asset bubbles, political instability and other risks.

Information Asymmetry and Professionalism

The banking world has built a wall of silence around their losses due to cybercrime, afraid of a loss of confidence in the banking system, if the true level of hacking impacts were made public. The amount of secrecy the world's banks have with regard to cyber hacking makes it difficult to address the problem fully and create effective regulations aimed at averting any possible financial crisis [f]. The banks themselves must acknowledge cyber hacking for the massive problem it is and to do their utmost to safeguard themselves and their clients. This behavior contradicts the basis of any transaction, i.e. both parties (banks and customers) must be treated fairly and their expectations (safety and security of their funds) met.

However, till the common man (bank customers) is not completely aware about the danger and the impact with which banks have been affected by cybercrime, there remains a lack of transparency, which implies that the banks are not being professional and are lacking integrity in their approach to control cybercrime. This Information asymmetry and lack of professionalism may in an extreme and unlikely scenario lead to people losing trust in traditional banks completely and maybe even moving to a barter system of trade.

Dynamic Nature of Attacks

Cyber-criminals have developed increasingly sophisticated forms of cyber-attacks regularly robbing financial institutions on a much larger scale. Hacking traditionally focused on stealing the login credentials of bank account holders either individuals or of small businesses. But the hacks are now targeting the banks and focusing on compromising their SWIFT accounts (like the case of Bangladesh Bank) or the attack on JP Morgan, in Oct 2014 where cyber attackers accessed the information of 76m households and 7m small businesses (no financial impact is reported yet). Customer data protection rules have become extremely strict and can cost companies massive fines and huge reputational losses.

The most, common form of cybercrime currently is ransomware: Malicious software that holds data files for ransom (via encryption) and demands (generally in crypto-currencies) a sum for returning data. As cybercrime flourishes there is a rising demand for crypto-currencies as it enables anonymous financial transactions. Since no central body can regulate crypto-currencies, transactions don’t have to go through a bank, credit union, or other agency allowing hackers the protection of anonymity while increasing both impact and frequency of cybercrime.

Incorrect Risk Control

The financial sector, as of today has not done enough to mitigate the risk of cybercrime, to take the example of the Bangladesh Bank, none of the involved parties have taken responsibility. Although Bangladesh bank’s security was compromised, both the Federal Bank and the SWIFT networks were used to carry out the heist. A key risk identified here is that the risk control measures should ideally be applied at the highest possible level which in this case would be the universal networks (SWIFT, IMF and World Bank) and branching to the network of central banks

like the Federal reserve system (the Fed), European Central Bank and other major national (central) banks, moving towards commercial and corporate banks, and then the smaller services like ATMs and e-wallet payment security. However this is not being done with all institutions focusing on internal security (to protect them) rather than protecting the entire system.

Cyber War-fare

The UK and USA made a joint statement blaming Russia for cyber-attacks on businesses and consumers in their economies, the National Cyber Security Centre (NCSC), US Department of Homeland Security and the FBI warn businesses and citizens that Russia is exploiting network infrastructure devices such as routers around the world. In order to carry out future attacks on critical infrastructure such as power stations and energy grids. China, North Korea and Iran are known to have dedicated cyber arsenals that are of increasing threat to the West with many major and minor incidents reported.

Reports suggests that cyber criminals could be paid to damage the economies of certain countries or sections of the worlds, possibly controlled by a foreign power, cyber criminals might simply wipe all records of a significant proportion of the West's wealth in order to create economic chaos and a financial meltdown. If this risk is not accurately mitigated then it could lead to a different type of world war, one that not many expect but could have more disastrous effects than maybe a nuclear war.

Lack of Insurance Protection and Pricing of Risk

A study conducted by Aon in 2015, estimated the cyber-insurance market is still in its infancy and penetration levels are still relatively low: less than 15% in the US and below 1% in other regions of the world [m], reiterating the fact that the market is significantly under insured because it cannot be priced accurately due to the following factors:

- Cyber risk has only emerged as a peril in recent years so no historic data (limited time-series data on incident frequency/impact) can increase parameter and model risk drastically.
- A potentially low share of cyber incidents are discovered and few incentives to voluntarily disclose incidents (and related impacts)
- Attacks are driven by human behavior rather than natural/physical forces
- Attack methods evolve/improve and respond to improvements in security measures
- Increasing exposures as reliance on digital technologies increases and a lack of diversification avenues for acquired risk
- Changing legal and regulatory environment (including liability/compensation practices) leads to changes in financial impact (complicated by differences across jurisdictions)
- Security of information on corporate defences creates a reluctance to share information between insured and insurer

High Impact Scenario

Since the world is not adequately prepared to face a global financial crisis triggered by cybercrime, it is an ideal example of a black Swan event (an event that has a very low probability of occurring but the expected loss can be extremely high).

So the next time a cause of global economic crisis is mentioned, cybercrime could either be the primary cause or a trigger event, but it has the potential to cause a financial crisis, and that is a fact. The global economy must take preventive measures immediately, else it may be too late and the economic environment around the world may never be the same.