RISK AND THREAT OF MONEY LAUNDERING THROUGH CYBERCRIME

Saturday,4th April, 2015

10 Most Notorious Money Laundering Cases of the 20th Century

1. **Pablo Escobar**
2. **President Suharto**
3. **Ferdinand Marcos**
4. **Meyer Lansky**
5. **Al Capone**
6. **Nauru**
7. **Franklin Jurado**
8. **The Benex Scandal**
9. **The BCCI Scandal**
10. **Sani Abacha**

1. The most successful criminal ever known, it has been said that at one point Pablo Escobar was so rich he spent $1,000 a week on rubber bands in order to wrap his bundles of cash. Escobar's business was drugs — at one time his cartel controlled 80% of the world's cocaine trade. Laundering money was central to Escobar's empire, and his recipe for success was relatively simple: "[Y]ou bribe someone here, you bribe someone there, and you pay a friendly banker to help you bring the money back." In 1989, Escobar's personal fortune was estimated at $9 billion, making him the seventh richest man in the world. His criminal career — and life — ended in 1993 following a gun fight with Colombian authorities.
2. Coming in at number one on Transparency International's most corrupt leaders list, Suharto was President of Indonesia from 1967 to 1998. After his forced resignation, Time Asia magazine estimated the Suharto family's wealth at $15 billion,
3. Ferdinand Marcos, an ex-lawyer, was president of the Philippines from 1965 to 1986 before being removed from power by a popular uprising. During his reign he laundered billions of dollars of stolen public funds through banks in the US and Switzerland. It took the Philippines a massive operation, known as "Operation Big Bird," to retrieve the money (estimated as US$7.5 billion).
4. made its way into "Benex Worldwide" accounts at the Bank of New York, one of America's oldest and most prestigious banks.
5. At its peak, the Bank of Credit and Commerce International (BCCI) was the seventh largest private bank in the world.

Al Capone

The best known of America's mobsters was at the forefront of the birth of modern money laundering schemes. It is estimated that he laundered $1 billion through various businesses. His first businesses were in fact Laundromats, which, being cash operated, were very helpful in hiding and disguising illegal gains. The fact that Capone made use of the laundry trade is frequently given as the origin for the phrase "laundering" — however this is still subject to debate. Capone was eventually indicted in 1931 for a different financial crime: tax evasion.

The term "money laundering" is said to have originated from the mafia ownership of Laundromats in the United States. The mafia earned huge amounts from extortion, gambling etc. and showed legitimate source (such as Laundromats) for these monies

Arrests made in $6 billion cyber money-laundering case

- Liberty Reserve, a major global online cash transfer business run out of Costa Rica, has been shut down and its executives arrested to face U.S. charges of laundering $6 billion
- Liberty Reserve was shut down over the weekend. According to the indictment, it had touted itself as the Internet's "largest payment processor and money transfer system." But authorities said it had never registered with the U.S. Treasury Department as a money transferring business, even though it had more than 1 million customers worldwide, including 200,000 U.S. customers. It handled 12 million financial transactions a year, according to the U.S Attorney

8 charged in $45 million cybertheft bank heist

- Federal prosecutors unsealed charges Thursday against an alleged cybertheft ring accused of stealing $45 million from banks around the globe and using the loot for Rolex watches, luxury cars and other booty

Scenes from a $45 million heist

- The ring used **prepaid MasterCard debit cards** that were issued by the National Bank of Ras Al-Khaimah PSC**, located in the United Arab Emirates, and the Bank of Muscat, located in Oman**
- The thieves hacked into the banks' **systems to drastically increase the amount available on the cards, and then used the information about the cards to withdraw money at banks around the world**
- He said the fact that the hacked banks were in the Middle East shows that cybersecurity in the global financial system is only as strong as the weakest link
- The eight suspects allegedly made nearly 3,800 separate transactions to withdraw the $2.8 million
- **During the first attack in December 2012, the New York group allegedly withdrew $400,000 in 750 separate ATM transactions at more than 140 different locations in New York City in less than three hours**.
- **Then in February, the perps withdrew $2.4 million in 3,000 ATM withdrawals made in just over 10 hours. Lynch described the group as a "virtual criminal flash mob, going from machine to machine drawing as much money as they can before these accounts are shut down**
- They deposited some of the cash into bank accounts, in one case putting almost $150,000 in $20 bills into one account.

EFFORTS

- The prosecutor, said her office worked with law enforcement authorities in 16 countries -- including Japan, Canada, Germany and Romania -- as part of the investigation
- "The defendants and their co-conspirators participated in a massive 21st century bank heist that reached across the Internet and stretched around the globe," said Lynch. "In the place of guns and masks, this cybercrime organization used laptops and the Internet."
- While hacking attacks often steal personal information that can then be used in identity theft schemes, hacking theft from banks and credit card companies by organized crime is also a growing problem. Two years ago, Citigroup (C) admitted that more than $2.7 million was stolen from 3,400 accounts during a hacking attack.

INDIAN SCENE

- In India, money laundering is popularly known as Hawala transactions.
- Hawala is an alternative or parallel remittance system. "Hawala" is an Arabic word meaning the transfer of money or information between two persons using a third person.
- The system dates to the Arabic traders as a means of avoiding robbery. It predates western banking by several centuries.
- The Hawala Mechanism facilitated the conversion of money from black into white.

FACTS

- As per IMF reports the turnover of this industry could be somewhere around $1.5 trillion.
- **320 million cyber attacks each day** Or
- **more than 3,700 attacks every second**
- Cisco also finds that 75 percent of all attacks take only minutes to begin data exfiltration but take much longer to detect
- **More than half of all attacks persist for months—even years—before they are discovered**
- And it can take weeks or months for a security breach to be fully contained and remediated

HOW, WHAT

- In all industries, efficient business models depend upon horizontal separation of production processes, professional services, sales channels etc. (each requiring specialised skills and resources), as well as a good deal of trade at prices set by the market forces of supply and demand. Cybercrime is no different: it boasts a buoyant international market for skills, tools and finished product. It even has its own currency.
- The rise of cybercrime is inextricably linked to the ubiquity of credit card transactions and online bank accounts. Get hold of this financial data and not only can you steal silently, but also – through a process of virus-driven automation – with ruthlessly efficient and hypothetically infinite frequency.
- The question of how to obtain credit card/bank account data can be answered by a selection of methods each involving their own relative combinations of risk, expense and skill.
- The most straightforward is to buy the 'finished product'. In this case we'll use the example of an online bank account. The product takes the form of information necessary to gain authorised control over a bank account with a six-figure balance. The cost to obtain this information is $400 (cybercriminals always deal in dollars). It seems like a small figure, but for the work involved and the risk incurred it's very easy money for the criminal who can provide it. Also remember that this is an international trade; many cyber-criminals of this ilk are from poor countries in Eastern Europe, South America or South-East Asia.
- The probable marketplace for this transaction will be a hidden IRC (Internet Relay Chat) chatroom. The $400 fee will most likely be exchanged in some form of virtual currency such as e-gold.

TOOLS – A QUICK VIEW

- As IT environments have increased in complexity, exploits have grown in sophistication
- And with significant money to be made, hacking has become more standardized, mechanized, and profit driven
- In the early 1990's, viruses targeted mainly operating systems. A decade later came self-propagating worms, which moved from machine to machine via enterprise networks and across the Internet. Spyware and rootkits – malicious software designed to gain privileged access to a computer and run stealthily – also emerged.
- Methods such as port and protocol hopping, encrypted tunneling, droppers, sandbox evasion, blended threats and techniques that use social engineering demonstrated increasingly sophisticated ways to penetrate networks.
- Today, attackers are more proficient than ever at discretely leveraging gaps in security to hide and conceal malicious activity.
- Snowshoe spam, spear phishing and malvertising campaigns are just a few examples of new ways that attackers are combining a savvy use of technology and IT infrastructure with a detailed understanding of user behavior to reach the intended target and accomplish the mission.

THE PLAYERS

- **Coders –** comparative veterans of the hacking community. With a few years' experience at the art and a list of established contacts, 'coders' produce ready-to-use tools (i.e. Trojans, mailers, custom bots) or services (such as making a binary code undetectable to AV engines) to the cybercrime labour force – the 'kids'. Coders can make a few hundred dollars for every criminal activity they engage in.
- **Kids –** so-called because of their tender age: most are under 18. They buy, trade and resell the elementary building blocks of effective cyber-scams such as spam lists, php mailers, proxies, credit card numbers, hacked hosts, scam pages etc. 'Kids' will make less than $100 a month, largely because of the frequency of being 'ripped off' by one another.
- **Drops –** the individuals who convert the 'virtual money' obtained in cybercrime into real cash. Usually located in countries with lax e-crime laws (Bolivia, Indonesia and Malaysia are currently very popular), they represent 'safe' addresses for goods purchased with stolen financial details to be sent, or else 'safe' legitimate bank accounts for money to be transferred into illegally, and paid out of legitimately.
- **Mobs –** professionally operating criminal organisations combining or utilising all of the functions covered by the above. Organised crime makes particularly good use of safe 'drops', as well as recruiting accomplished 'coders' onto their payrolls.

WHY THE THREATS

- Attackers' techniques are highly sophisticated and often go to extraordinary lengths to mount an attack, following a series of steps known as the "attack chain," a version of the "cyber kill chain." It's not uncommon for hacker groups to follow software development processes, like QA (quality assurance) testing or bench testing their products against security technologies before releasing them into the wild, to ensure they'll evade the defenders.
- Long before they actually execute an attack, hackers enter into the target organization's IT infrastructure, conducting recon using surveillance malware. Only when they know what they're up against do they write target-specific malware targeting specific departments, applications, users, partners, and security processes. To ensure the malware works, malware writers recreate an environment to test it against security tools. Some even offer guarantees that their malware will go undetected for weeks or months.
- As organizations embrace BYOD policies, cloud computing, and mobility initiatives, gaining visibility, improved context into connected users and devices, and effectively enforcing security policies becomes more imperative. Security experts predict that CISOs will increasingly turn to more sophisticated endpoint visibility, access, and security control solutions to manage the complex web of connections among users, devices, networks and cloud services.

WHATS TO BE DONE

- In addition, organizations need to employ a threat-centric and operational security model that is focused on the threats themselves versus just policy or controls.
- Organizations need to look at their security model across the extended network and the full attack continuum—before an attack happens, during the time it is in progress, and after it gains access to the network. They need to be able to respond at any time, all the time.

The Preventive Implementation by the Financial Institutions

- The technological products such as prepaid cards, e-cash, swipe cards, e-gold and online banking has introduced a number of opportunities for the criminals to hide their identity or use some one else's identity to do a transaction and get away with it before being catch
- Financial institution are required to submit suspicious activity report to the financial monitoring agencies and
- Also required to know their customer through customer due diligence also called know your customer (KYC)
- Suspicious transaction means that a customer transaction that does not fit into his profile or a foreign transaction that is relatively unusual

Different ways to achieve Cyberlaundering - DIRECT

- Cyberlaundering can be achieved through directly interacting with the financial institution by presenting the identity in a way to hide the real intent (i.e. Cyberlaundering)
- Through that financial institution. There are five classes of such dealings that are classified in relation to the issue of Cyberlaundering and are given as follows
- “Concealment within Business Structures; Misuse of Legitimate Businesses; Use of False Identities, Documents, or Straw Men; Exploiting International Jurisdictional Issues; Use of Anonymous Asset Types;

CYBERLAUNDERING - INDIRECT

- However there is another way of achieving Cyberlaundering and is termed as indirect way or a way to avoid direct dealing with the financial institution to protect the transaction from being reported to financial agencies and that is the hawala system or alternate banking remittance. In addition to this system of remittance there are other products that can be used to achieve Cyberlaundering and they are listed as follows.
- "E-Cash, Online Auctions, Bankruptcy frauds, Telemarketing fraud, Operation Cyber Sweep, Cyber terrorism, Online Banking, Iraqi internet scam, E-gold and Online Casinos"

THE PROCESS

- Stages of the Process of Cyberlaundering
- The process of Cyberlaundering can be achieved by the three stages which is in contrast to its super set that is money laundering and the three stages such as placement, layering and integrity are explained below

STAGE 1 - PLACEMENT

The illegal money in the form of smart cards can be used in online casinos or to buy e- gold without even proving that the identity is authentic, this can be a source to convert dirty money in to legitimate in the form of refund from a casino in the same area or in a different area where the jurisdiction is less tolerant or have no check on the gambling activities

STAGE 2 -LAYERING

- In the stage of layering the criminal tries to separate the money from its origin by transferring the money through a number of accounts in different banks in the disguise of purchase of goods for re-sale or through off shore companies located in different jurisdictions.
- In this stage the criminals are more likely to be facilitated by the use of internet which if permits to open an account without linking to any authentic proof of identity and any traditional bank account. With this features the criminals can hide there identity or they can use a fake identity to open a bank account.
- The transfer of funds from one jurisdiction to another leaves extensive audit trails. But the investigation in to a transaction to be legitimate requires a lot of man power and time compared to the instantaneous nature of the electronic transfer of money.
- Layering could be achieved much easier if the bank supports transfer of funds that deal with e-money. Then the source of income is virtually untraceable for some types of e-money transaction using the anonymity features that available with most of the plastic cards available in the market

STAGE 3 -INTEGRATION

- In the stage of integration the owner need to make sure that the accumulation of illegal wealth should not appear to be so; rather it should appear legitimate
- There are a number of ways to achieve that, the traditional way involves false invoices of goods while the other way is to open a shell company that render a service such as internet service provider

STAGE 3 – NEXT STEPS

- Open a bank account for this shell company and you don't even need to render service but rather use this shell company to make it appear that the services are being provided in return of payment of funds that have passed through layering process
- This way the wealth of the owner looks legitimate which can be said as the profit of the service provider
- The later technique to provide a legitimate appearance to the funds has a greater scope then the traditional technique
- As the traditional technique would require to be of limited use as the services can only be rendered in a limited geographical location while the internet service provider can be bared from this limitation and hence the profits can be far more then the traditional technique
- One more benefit to opt for the later technique is the reduced suspicions if the funds are transferred from foreign banks

WORLD BANKS VIEW

A World Bank article described four models of cyber based payment systems the system that is growing exponentially and that facilitates the money laundering capabilities is the non-bank and peer-to-peer model. The four models are as follow:

MODELS FOR CYBERLAUNDERING

- The Merchant Issuer Model: This model deals with the case of same entity that is both the issuer and the seller.
- The Bank Issuer Model: This model deals with the case that the issuers are separate entities from the merchant. This model is connected with the traditional financial system. E.g. Debit card used by account holders of any bank.
- Non-Bank Issuer Model: This model deals with issuer giving e-cash in exchange of traditional funds and spending this e-cash at participating merchants. E.g. FOREX CARDS
- Peer-to-Peer Model: This model deals with e-cash that is transferable between users. Point of contact with the transitional financial system is when the e-cash is issued and when it is redeemed. E.g. PayPal funds transfer services

MODUS OPERANDI

- The criminals can easily avoid such restrictions by opening online accounts with so many unregulated electronic banking companies that use electronic payment systems to provide online banking like functionalities with the added layer of hidden transaction.
- With the introduction of prepaid cards the criminals can be utilizing the anonymity feature of the card to help the layering and integrity stage of Cyberlaundering.
- The peer to peer model of the payment system enables the criminal to move the electronic cash from one card to another card without even getting any attention from the law enforcement agencies and without the need to report such transaction by the unregulated online bank

To Conclude

- In 2001, U.S. prosecutors obtained almost 900 money-laundering convictions with an average prison sentence of six years. The rise of global financial markets makes money laundering easier than ever. Countries with bank-secrecy laws are directly connected to countries with bank-reporting laws, making it possible to anonymously deposit “dirty” money in one country and then have it transferred to any other country for use. Depending on which international agency you ask, criminals launder anywhere between $500 billion and $1 trillion worldwide every year. The global effect is staggering in social, economic and security terms

- Terrorist funds are recycled in the financial system through a variety of layering techniques which take advantage of regulatory and supervisory weaknesses. Most recently the UK stated that financial crime there was 2% of GDP

Steps Taken so far

- Fighting money laundering in cyberspace is a totally different ball game. There are process-oriented and technological weapons against cyber laundering. Here are some of the process- and policy-oriented means :

- **FSAPs**— The World Bank Group has incorporated a dedicated anti-money laundering module into the Financial Sector Assessment Program (FSAP). This module can be enhanced by updating it to provide technical assistance and training on how to identify and reduce new means of money laundering, cyber-crime and terrorist financing such as the "Non-Bank Issuer Model" and the "Peer-to Peer Model".
- **Global Payments Systems Mapping Project**— Operational risk is a constant of doing business in a globally interconnected environment. By mapping the various means by which money moves, it will be possible to identify patterns, trends and discrete relationships otherwise unnoticed. This project and the knowledge derived there from can grant policy makers a better understanding of the flow of money, which can in turn be converted into knowledge for helping nations craft such things as monetary policies and financial risk assessment models.
- **FATF Principle #13**— Knowledge of one's customers is a fundamental requisite to prevent money laundering. The "KTC" principle is significantly hampered by online transactions where digital money and anonymity of users creates a highly stealthy environment. To increase transparency, there are many authentication solutions, including the use of biometric and public key infrastructure (PKI) for users who initiate large value transfers. Two-factor authentication should be mandated by law for all financial transactions.

Indian Scenario...

- Out of 140 countries, India has been ranked 93rd and 70th in 2012 and 2013 respectively with a score of 6.05 in 2012 and 5.95 in 2013, as compared to Norway, which has a score of 2.36 and ranks No. 1 in the Anti Money Laundering (AML) Basel Index 2013.

- AML Basel index is country risk ranking which focuses on money laundering/ terrorist financing risk, consisting of 14 indicators of assessment.

- This clearly shows that India, in the present-day scenario, is very vulnerable to money laundering activities and is a high risk zone.

- India needs to curb Money laundering as the practice is rampant across the country. It is estimated that a total of $343 billion has been laundered out of India during the period 2002-2011.