CREDIT CARD FRAUD: A RISING THREAT TO GLOBAL BANKING INDUSTRY

The credit cards frauds are rapidly increasing since the day, the credit card were launched. With the continuous change in the technology, doing transaction over the internet has become part and parcel of the daily life and as such credit cards become more sophisticated incorporating various features for security as well as ease of use. The race is continuous among banks/industry introducing various horizontal and vertical laws and other regulations such as PCI-DSS, ISO 27001 etc. to control the cyber frauds and at the same time, fraudsters/hackers adopting new methodologies to commit the crime as surfaced in recent Kotak Mahindra Bank credit card fraud.

With the exponential growth of e-commerce coupled with all the countries moving towards E-Governance, the demand for credit card transactions have increased and at the same time, the credit card fraud have increased multi folds and claims to $US465 billion a year in 2015. The hacker/fraudsters have targeted to by-pass all the identity and access management controls in order to steal the data which is required for committing the offence. The movement of the companies towards cloud computing have resulted into shifting of Identity & Access Management to Identity-As-A-Service (IdaaS). The huge online traffic and also globally spread users have forced all the big portals like google, facebook etc. to move the Identity & Access Management towards IdaaS whereby it become feasible to cater these users through redundant/fault tolerance server on the web. This new network architecture has created the ample scope for the fraudsters and coupled with the evolution of the virtual currencies make it easy to transfer the proceed of crime globally with any remote chance of success to the law enforcement agencies.

The recent scam of the Kotak Mahindra Bank wherein a massive fraud was detected in which 1,730 transactions worth Rs 2.84 crore were executed using credit cards which was never issued. The 580 cards were fabricated by the fraudsters and used for online shopping and making payments in seven countries - Canada, USA, UK, Germany, Brazil, France and India - between July 2 and September 10. The manner in which the scam has been reported to be committed raise serious question on the in-built security mechanism sought to be enforced including ISO 27001, PCI-DSS Guidelines, RBI Regulatory Guidelines etc.

The scam clearly indicates the involvement of insiders as the credit cards have been alleged to be issued in the name of non-existing persons and as such the questions arises from where these forged data have entered into the system, who verifies their identity, their address proof and how the forms would have been forged. This raises serious question of compliance with PCI-DSS which provides the security architect with a framework of specifications to ensure the safe processing, storing, and transmission of cardholder information. PCI-DSS is focused on compliance with the standard that includes prevention, detection, and reaction to security incidents. PCI-DSS controls specifically require the corporate entity to maintain vulnerability management program, Implement strong access control measures, Maintain an Information Security Policy.

The RBI Guidelines and Information Technology Act, 2000 also requires the bank to comply with the ISO 27001 which contains the large number of controls to be intertwined into the system architecture so as to control the flow of data, transactions and stipulates strong access controls which are required to be audited by the Information System Auditor. The modus operandi of the credit card fraud of Kotak Mahindra Bank shockingly raises the issues of efficacy, efficiency, effectiveness of these controls and it would be up to the Investigating Agencies to see whether these controls were in place or not and to fix the liability of the offenders in terms of Section 85 of the Information Technology Act, 2000.

The fraud has been committed through online transactions scattered over a number of countries pointing towards involvement of International Mafia. The suspicious entities in the global network exist which allows execution of transactions even without any password and solely on the basis of credit card information such as Credit Card Number, CVV/Security Code, Date of Expiry, Name of the Card Holder etc. The International Mafia play a pivotal role in converting the proceeds of these transactions to the virtual currencies like Bit-coins and through multi-layering, the trail of the money goes into the dark web and cannot be detected.

The ease of doing the credit card frauds coupled with the dim chances of prosecution have made the credit card fraud as one of the lucrative industry and the young generation is moving into this arena which provides easy money with no risk. Further, the incapability of the police to investigate such crime and to collect the relevant evidence have resulted into either no detection or without any sufficient evidence resulting into free breathing space for the credit card fraudsters.

Though the Indian Banks particularly private sector banks are spending a lot in terms of security by installing Firewalls, Proxies, UTM etc. but the recent Cyber breaches such as Sony Hack, Target, JP Morgan, Morgan Stanley etc. indicates that the security technologies play a limited role in protecting the infrastructure. The crucial element is the person behind these devices to be trained, efficient, knowledgeable to apprehend such threats and take appropriate counter measures.

Tags – Credit Card Fraud, ISO 27001, PCI-DSS, IdaaS, Access Control, Information Security Policy, Information Technology Act, 2000, Bit Coin, Cyber Breaches