Abhishek Honmute
111803055
Div 1 Batch B2
Cyber Security
Assignment 2

Case Study On Latest Cyber Crimes

Case I: Pune Citibank MphasiS Call Center Fraud

Incidence:

US $ 3,50,000 from accounts of four US customers were dishonestly transferred to bogus accounts. Some employees gained the confidence of the customer and obtained their PIN numbers to commit fraud. They got these under the guise of helping the customers out of difficult situations. The highest security prevails in the call centres in India as they know that they will lose their business. There was not as much of a breach of security but of sourcing engineering. All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to Pune accounts and that's how the criminals were traced. Police have been able to prove the honesty of the call centre and have frozen the accounts where the money was transferred.

Applicable Law:

Under ITA-2000 the offence is recognized both under Section 66 and Section 43. Accordingly, the persons involved are liable for imprisonment and fine as well as a liability to pay damages to the victims to the maximum extent of Rs 1 crore per victim for which the "Adjudication Process" can be invoked.

Case II: Cosmos Bank malware attack

Incidence:

It was India's one of the biggest cyber-attacks. Hackers hacked into the bank's ATM server and took details of many visas and rupee debit cardholders. Stolen data was used to create cloned debit cards of cosmos bank, which were used for thousands of ATM transactions from India and 28 other countries in a period of 7 hours on August 11, 2018. While around Rs 78 crore was withdrawn in more than 12,000 ATM transactions outside India, another 2,800 transactions of Rs 2.5 crore were made in different places in India. Further, on August 13, 2018, more Rs 13.92 crore were transferred to a Hong Kong-based entity using Society for Worldwide Interbank Telecommunications (SWIFT) facility. The transactions outside India were done through Visa cards, those in India through RuPay cards, a probe has shown.

Applicable Law:

A total of Rs 94 crore was siphoned off in this case, which was registered at the Chaturshringi police station under sections 120B, 420, 467, 468, 469, 471, 34 of the Indian Penal Code and relevant sections of the Information Technology Act. This kind of crime comes under Section 66 - Hacking.

Case III: Syed Asifuddin and Ors vs state of Andhra Pradesh and ANR

Incidence:

The instant case was registered on basis of a written complaint of the Head of Sales and Marketing wing of M/s Reliance Infocomm Ltd, Hyderabad (Respondent No. 2). Reliance Infocomm had launched telephone services called 'Reliance India Mobile', later modified to 'POBF'. The subscriber would get a digital handset exclusively franchised to Reliance and Reliance mobile service bundled together, for three years. It's been alleged that the subscribers of Respondent No. 2 were being attracted by other service providers through phone calls informing them of better tariff plans and services and the option to shift service providers. Once subscribers wanted to shift their mobile service provider, the petitioners hacked the Electronic Serial Number (ESN)by reprogramming it. As the Mobile Identification Number (MIN) of Reliance handsets were irreversibly integrated with ESN, re-programming the ESN ensured the device would be validated/authenticated by the Petitioners' service provider and not by Reliance Infocomm's device.

Applicable Laws:

These kinds of crimes come under Section 65 - Tampering with Computer Source Documents. The government arrested a few of the Tata Teleservices Limited officials for reprogramming the reliance handsets.