ABA Policy Advocacy Committee
Preventing Data Compromise

Dilshan Rodrigo

ABA Conference, Maldives

16th Nov ‘18

Data Leakage issue
September 2017

How can data be compromised

- Inconsistent and incompatible security practices, standards of party vendors and outsourced service providers (e.g. statemer printing, bulk marketing promotions, customer files to auditor
- Loopholes with evolving technologies and connecting digital platforms (e.g. swift, pickme, uber etc..)
- Weak controls with information sharing with related companie
- Man in the middle vulnerabilities (ie. Phishing, POS trxs)
- Heightened info security threats – vulnerable countries in Glob Cyber Security Index
- Delays in security patch management for exposed environmer servers in DMZ)

Recent vulnerabilities in the Banking Indu

- In Feb 2016, hackers broke in to **Bangladesh Bank** and hacked its credentials to send p over SWIFT network. They stole $81mio. (a custom malware developed by an alliance a software running in Bangladesh Infrastructure
- **Well Fargo** accidently leaked 50,000 private banking customers data in July 2017 includ spreadsheets with customer names and social security numbers, paired with size of inv portfolios and fees the bank charged them
- **Far Eastern International Bank i**n Taiwan was hacked by state sponsored North Korean criminals wired $60mio to destinations such as Sri Lanka, Cambodia and USA. Based on intelligence first direct interaction of the bank began with spear phising attacks that co malware attachments
- **Equifax** an American credit card company revealed that it has suffered a major cyber a July 2018. Personal data names, birthdates, social security numbers driving licences of American, British and Canadian customers were affected as well as 200,000 credit card

How to prevent such compromises

Administrative Controls

- Setting the tone at the top – CISO Role
- Regular security reviews of systems (pen testing, ethical hacki
  vulnerabilities, alerts etc..)
- Bank wide data classification
- Certifications – ISO 27001 for Data Centre, DR and IT Departm
- Restrict email dissemination, no external memory drives, attac
  must carry passwords
- Strengthen Data Warehouse standards for data dissemination
- Regular IT Security awareness for staff, Reviews and Incident

How to prevent such compromises

Technical Controls

- External vulnerabilities protected by firewalls
- End point Anti virus and Anti Spam solutions
- POS protected by Terminal Line Encryption
- 3D secure for eCommerce applications for IPG
- 2FA and PAM to protect eBanking Transactions and only act or
  mail for third party transactions
- EMV chip enabled Credit and Debit Cards
- Audit Vault to monitor unauthorized backend tier 1 – DB upda

How to prevent such compromises

Other

- Plan for a SOC to achieve continuous surveillance and real tim
  analytical capabilities
- Cyber Crisis Management Plan
- Cyber risk insurance