EBAday 2015

Boardroom focus: Financial crime and security in payments

Moderator:

- André Vink, EBA CLEARING

Speakers:

- John Flynn, Global Head of Anti-Fraud & Investigations, Deutsche Bank
- Gerard Hartsink, Chairman of the Board, Gleif

Finextra

ABE EBA
EURO BANKING ASSOCIATION

EBAday 2015

Financial crime and security in payments:

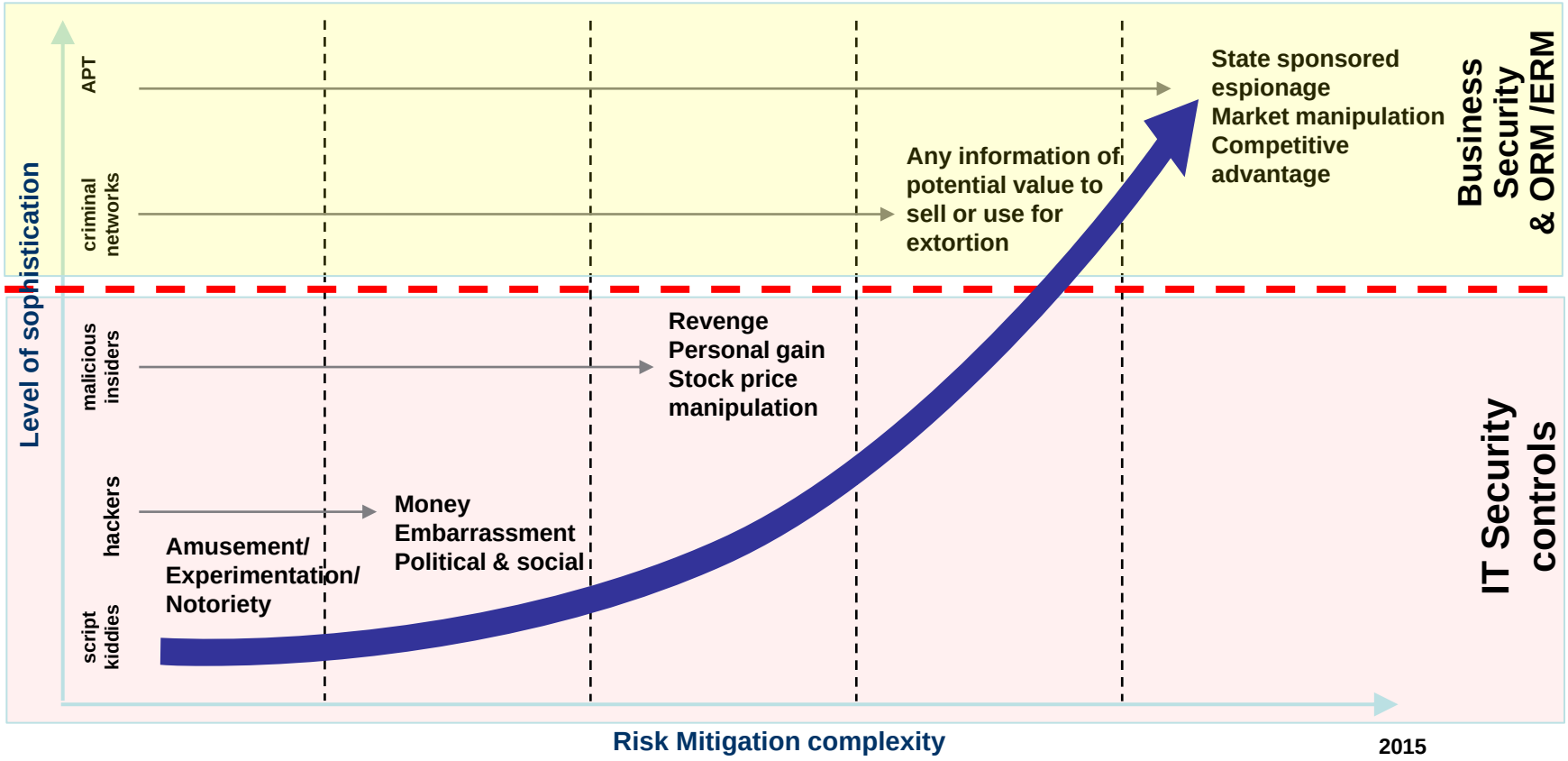
‘What the hack?’

Finextra

ABE EBA
EURO BANKING ASSOCIATION

The changing landscape of cyber threats: *Deal with "Financial Crime 2.0"*

The funding, organization and capability of "criminals" carrying out cyber attacks is increasing at an astonishing speed. Attacks are more sophisticated than ever, and it's not "just go and get the money" anymore – today we need to deal with a new generation of Financial Crime threat, covering the full spectrum of business operations (from IT to payments to market manipulation to data).



Source: EY GISS 2014

Financial crime and security in payments

John Flynn, Global Head of Anti-Fraud & Investigations, Deutsche Bank

EBAday 2015
10TH ANNUAL CONGRESS

Finextra

ABE EBA
EURO BANKING ASSOCIATION

Current situation

- Increasing Cybercrime attacks
- Targeting Corporate Customers
- Barriers to entry are low – Laptop and knowledge
- Return on investment – good
- Ease of being a victim
- Low risk of identification by law enforcement
- Use of multiple jurisdictions to move funds which results in cross border investigations – which frustrates detection and asset tracing
- Cybercrime is still concentrated in the more developed countries due to infrastructure
- Credentials obtained through Social Engineering – phishing and malware attacks

- Has data become the most valuable commodity?

Challenges for Banks

- Clients want faster, easier banking with multiple connection options
- Many banks have complex and aged IT systems which may present problems when embedding effective security measures
- Interconnections between firms are increasing as we place greater reliance on each other
- The cost of managing the risk of cybercrime will increase as more business functions become digital

- Authenticating the customer is going to be one of the greatest challenges

  Three key components
  - Knowledge – something the customer only knows – static password, personal ID number
  - Ownership – something only the user possesses – token, smart card
  - Inherence – something the user is – fingerprint, biometric characteristic

  Secure access is going to be reliant on a combination of the above

Response and Best Practice

- Risk Assessment
- Incident monitoring and reporting
- Risk Controls
- Traceability and Communication
- Customer identification
- Authentication of the customer
- Transaction Monitoring
- Response plan

Also need

- Engagement of Executive Management Team and ensure that they are aware of the risks and necessary steps required to combat them
- The organisation must be dynamic and flexible in responding to the changing threat
- Willing to share information with other banks

Financial crime and security in payments

Gerard Hartsink, Chairman of the Board, Gleif

EBAday 2015
10TH ANNUAL CONGRESS

Finextra

ABE EBA
EURO BANKING ASSOCIATION

EBAday 2015

Financial criminals

- Fraudulent merchants
- Fraudulent customers
- Fraudulent intruders of payment systems
- Fraudulent staff of PSPs and merchants etc.

Risk mitigation

- Risk mitigation in a three layer structure
  - PSP services to customers: competitive space
  - Scheme layer (SCT, SDD and Cards): cooperative space
  - Processing and communication: competitive space
- End to end approach essential
- Schemes have a prominent role in risk mitigation
- Schemes could mitigate risks by including the LEI
  - CSM (direct and indirect participants)
  - Payment page of web merchant
  - Mandate of Direct Debit

EBAday 2015

Multiple points of potential attacks in the customer to bank space

- User ID and device theft
- Device hacking
- Application tampering
- SIM spoofing
- Man in the middle attack

Cooperation of the public and private sector is mission critical

- Strong oversight by central banks on payment and card schemes is beneficial to enforce security in payments
- Principle 17 Operational Risks of the CPMI-IOSCO Principles (April 2012)
- Cyber Resilience for FMIs (CPMI Nov 2014)
- ICC Cyber Security Guide for Business (April 2015)
- PCI Data Security Standard

EBAday 2015

Thank you to speakers

- André Vink, Chief Risk Officer, EBA CLEARING
- John Flynn, Global Head of Anti-Fraud & Investigations, Deutsche Bank
- Gerard Hartsink, Chairman of the Board, Gleif

Finextra

ABE EBA
EURO BANKING ASSOCIATION