The cyber-threat and financial stability

Rohini Tendulkar
Economist
International Organization of Securities Commission

Disclaimer

The views and opinions presented in this presentation are those of the presenter only and do not necessarily reflect the views and opinions of IOSCO or its individual members.

Introduction

An emerging risk: **Cyber-crime or 'the cyber threat'**

IOSCO Research Department definition:

"a harmful activity, executed by one group or individual through computers, IT systems and/or the internet and targeting the computers, IT infrastructure and internet presence of another entity."

Introduction

"Sure cyber-crime is a nuisance but is it really a serious threat to financial stability?"

Content

I. The cyber-threat to the financial system: tackling the myths

II. Survey to the world's exchanges

III. Measures and responses

Content

Myth #1:
Perpetrators of cyber-crime in the financial system are simply criminals looking for financial gain

=

Motives

- Thieves/fraudsters looking for financial gain.
- 'Hactivists', motivated by a political ideal or ideology.
- Cyber spies, stealing political or economic secrets from firms and nations.
- Nation states or terrorist groups, using the cyber vector to disrupt or destroy.
- Insiders seeking to steal or sabotage.
- Individuals looking to wreak havoc for fun.

Targets

- Money
- Information
- Critical systems

Myth #2:
Cyber-crime is a passing nuisance

=

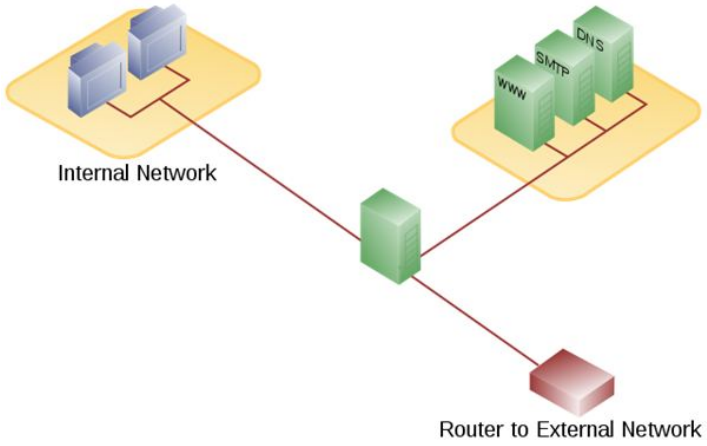
… a growing threat

- Potential to reap massive reputational damage across whole sectors
- Debilitating effects on market availability and integrity.
- A potential systemic risk.

"This is a rapidly rising area of risk with potentially systemic implications."

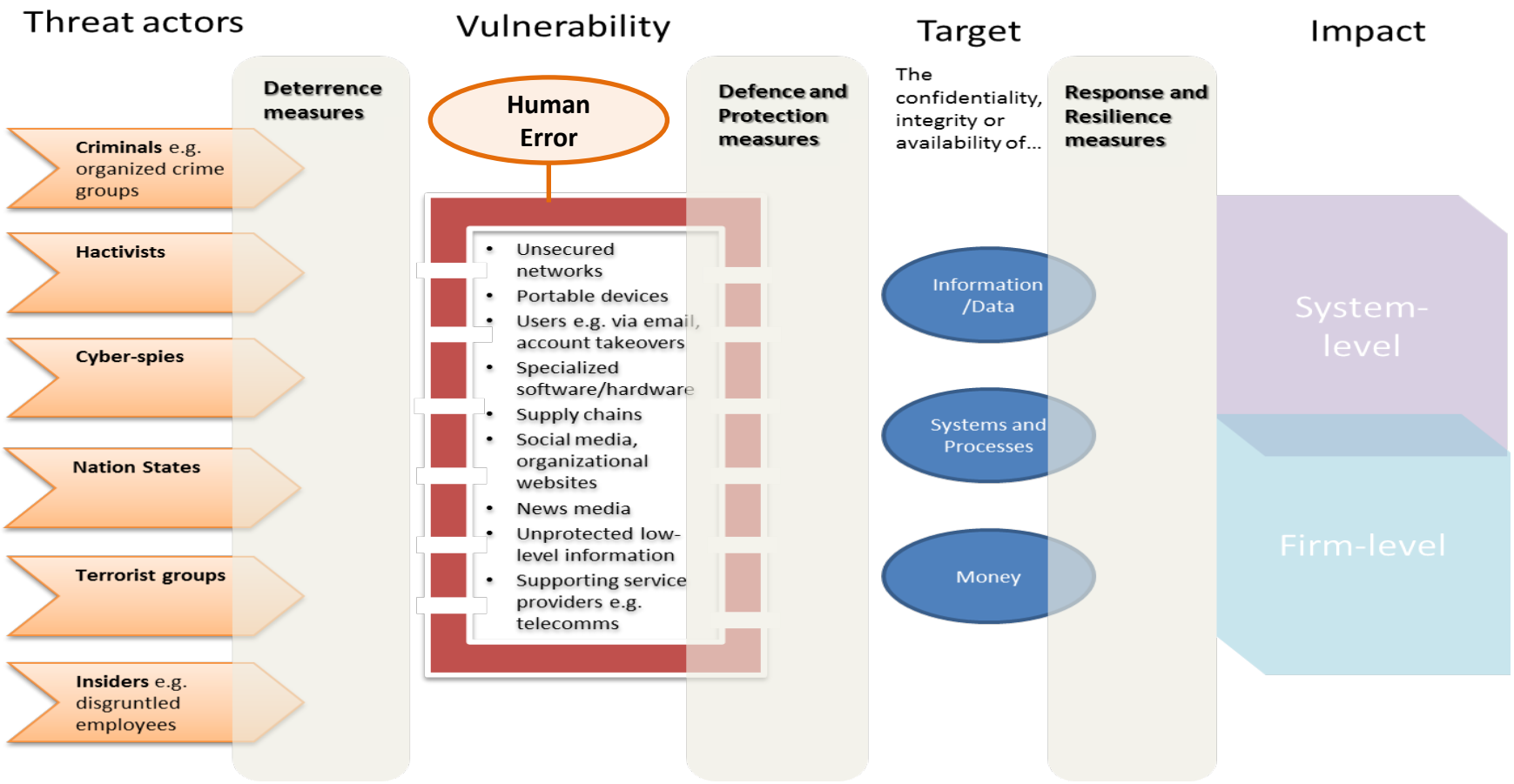
-- Andrew Haldane, executive director of financial stability at the BoE

Myth #3:
Cyber-crime is an IT issue



=

Vulnerabilities



Source: IOSCO Research Department

Content

I. The cyber-threat to the financial system: tackling the myths

II. Survey to the world's exchanges

III. Measures and responses

Cyber-crime and systemic risk

See report 'Cyber-crime, Securities Markets and Systemic Risk':
www.iosco.org/research

- Impact factors to inform analysis:
  - Size of the threat
  - Complexity
  - Incentive structure
  - Effect on market integrity and efficiency
  - Infiltration of non-substitutable and/or interconnected services
  - Transparency and awareness
  - Level of cyber-security and cyber-resilience
  - Effectiveness of existing regulation

Case Study: the World's Exchanges

- Size of the threat, complexity of attacks

53% of exchanges reported suffering a cyber-attack(s) in 2012.

A mix of simplistic (e.g. DDOS) and sophisticated (e.g. malicious code) attacks .

- Motive, effect on market integrity and efficiency, attacks on non-substitutable and/or interconnected services

Majority of attacks disruptive in nature.

Attacks against exchanges which are non-substitutable infrastructure and heavily interconnected.

No impact on market integrity and efficiency…. yet.

Case Study: the World's Exchanges

- Transparency and awareness

93% of exchanges report that cyber-crime is generally understood and discussed by senior management

89% of exchanges report having a formal plan/documentation addressing cyber-threats

70% of exchanges share information with authorities, regulators and other actors – on a national basis.

Case Study: the World's Exchanges

- Level of cyber-security and cyber-resilience

All exchanges have detection and preventative measures in place.

94% have disaster recovery measures in place for cyber-attacks.

85% of exchanges have training for general staff

89% of exchanges report having a formal plan/documentation addressing cyber-threats

70% of exchanges share information with authorities, regulators and other actors – on a national basis.

Perception that a large-scale attack with potential for widespread damage will eventually breach.

22% have cyber-crime insurance or something similar.

Case Study: the World's Exchanges

- Effectiveness of existing regulation

59% report sanction regimes in place for cyber-crime

Of these only half suggesting these are effective in deterring cyber-criminals.

Doubt due to cross-jurisdictional nature of cyber-crime and issue of attribution.

Case Study: the World's Exchanges

A systemic risk?

89% of exchanges view cyber-crime as a systemic risk.

- Halting trading activity or affecting the ability of a clearing house to act as a central counter party within the settlement window
- Moving markets through takeover of accounts and unauthorized trading
- Targeting telecommunication networks supporting financial structures
- Ongoing data manipulation and compromise of financial data integrity
- Leaking of insider information on an ongoing basis
- Attacking multiple, interconnected financial actors in different jurisdictions simultaneously

Question

"Sure cyber-crime is a nuisance but is it really a serious threat to financial stability?"

"This is a rapidly rising area of risk with potentially systemic implications."

-- Andrew Haldane, executive director of financial stability at the BoE

"It's a big deal; it's going to get worse"

-- Jamie Dimon, CEO of JP Morgan

"The financial services industry is one of the more attractive targets for cyberattacks, and, unfortunately, the threat is growing"

-- Thomas Curry

"This issue has emerged as arguably the top systemic threat, facing not only the global financial markets and associated infrastructures, but also world governments and military establishments."

-- DTCC, Beyond the Horizon White Paper, Aug 2013

"Will the next systemic shock spring from a liquidity crunch or inherent capital weakness… or is it more likely to come from an as yet unforeseen event or network of events such as a massive payment outage or a new breed of cyber attack?"

-- KPMG

Content

I. The cyber-threat to the financial system: tackling the myths

II. Survey to the world's exchanges

III. Measures and responses

Measures and Response

A system-level response:

(1) harmonizing fragmented approaches to cyber-crime across jurisdictions and supporting efforts in emerging markets.

(2) facilitating cross-jurisdictional information sharing on attacks.

(3) Providing a repository of knowledge for securities market participants to tap in to.

(4) developing principles for cyber-security and resilience and also for regulation to deter cyber-criminals.

(5) considering emergency response guidelines to deal with successful large-scale cyber-attacks on securities markets.

Questions?

Rohini Tendulkar
Economist
International Organization of Securities Commission