



Cyber-threat: survey to exchanges

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.

Content

- I. **IOSCO's focus on cyber-crime**
- II. **Survey to the world's exchanges**
- III. **Further work**

Content

- I. **IOSCO's focus on cyber-crime**
- II. **Survey to the world's exchanges**
- III. **Further work**

A growing and potentially systemic threat...

- ... in a complex and interconnected financial system
- ...where trust and confidence is key
- ... and financial actors are increasingly relying on technological innovation.

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

IOSCO Research Department definition:

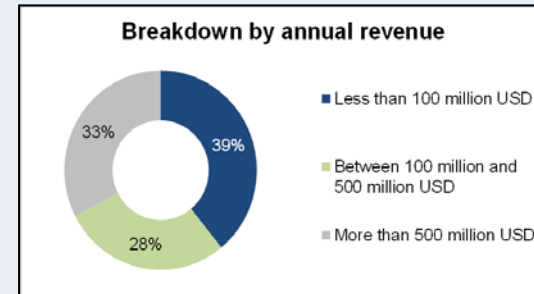
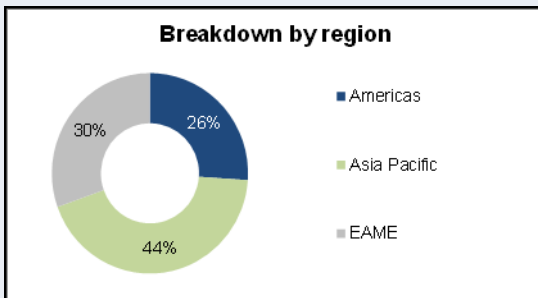
“a harmful activity, executed by one group or individual through computers, IT systems and/or the internet and targeting the computers, IT infrastructure and internet presence of another entity.”

Content

- I. The cyber-threat to the financial system: tackling the myths
- II. Survey to the world's exchanges
- III. Measures and responses

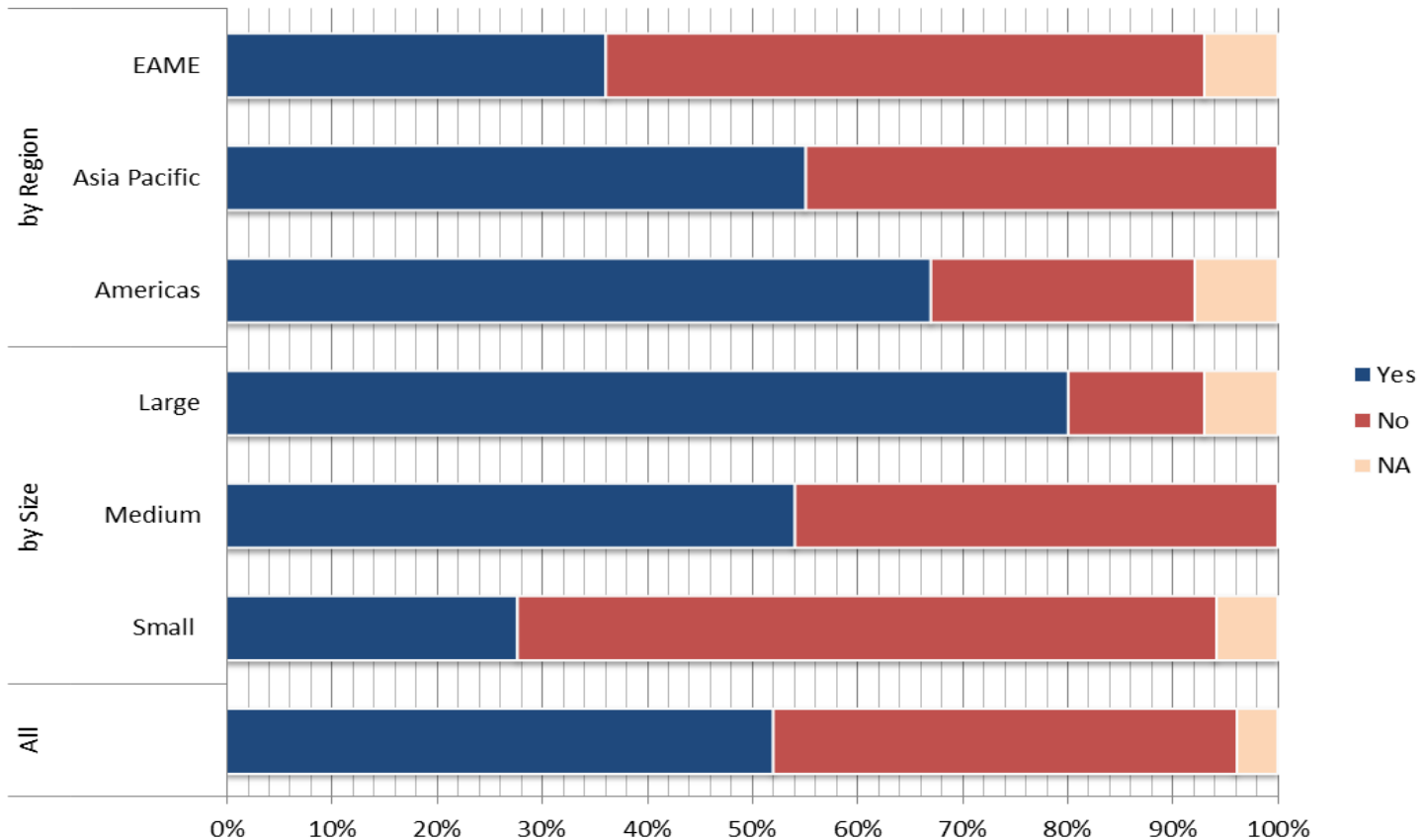
Survey to the world's exchanges

- The survey asked 23 quantitative and qualitative questions covering organizational approaches to cyber-crime; cyber-crime statistics; preventative and recovery measures; information sharing; views on policy and regulation; and insights on the systemic risk aspect of the threat.
- The survey questions based on market intelligence with cyber-security experts and market participants. A pilot survey was also sent out to a small, selected group of exchanges to confirm feasibility and appropriateness.
- **The final survey received 46 responses, constituting a 75% response rate.**
- Small exchanges have been classified for the purpose of presenting the results of the survey in this paper, as those with an annual revenue of less than 100 million USD. Medium-sized exchanges are those with annual revenue between 100 and 500 million USD. Large exchanges are those with more than 500 million USD annual revenue.
- Regions have been broadly divided into the Americas, Asia Pacific and Europe, Africa and Middle East (EAME) for anonymity purposes.



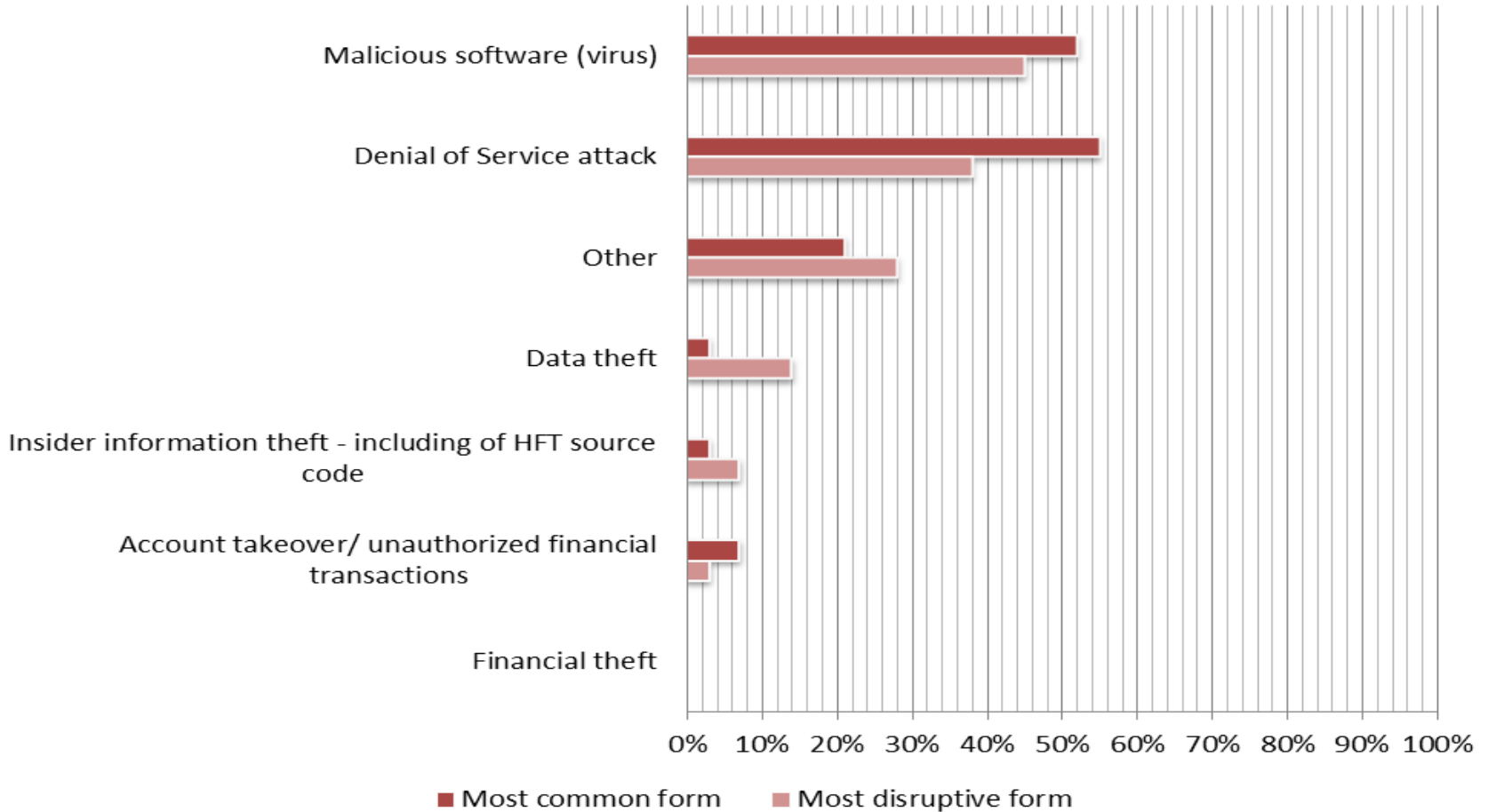
A global and universal problem...

Has your org suffered a cyber-attack in the last year?



...and attacks are mostly disruptive in nature

Most disruptive and most common form of attack?



... it can be considered a potential systemic risk

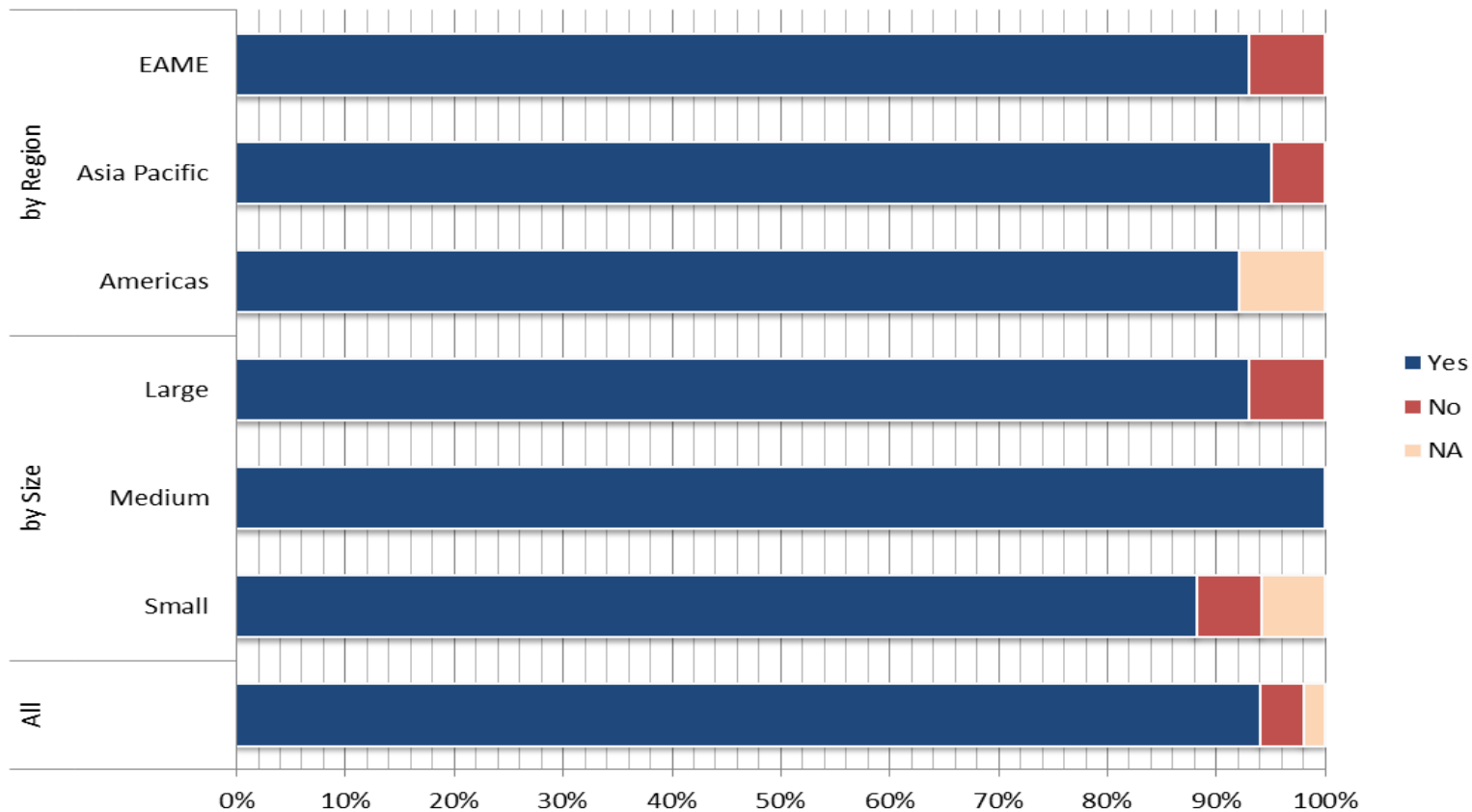
A systemic risk?

89% of exchanges view cyber-crime as a systemic risk. E.g. through:

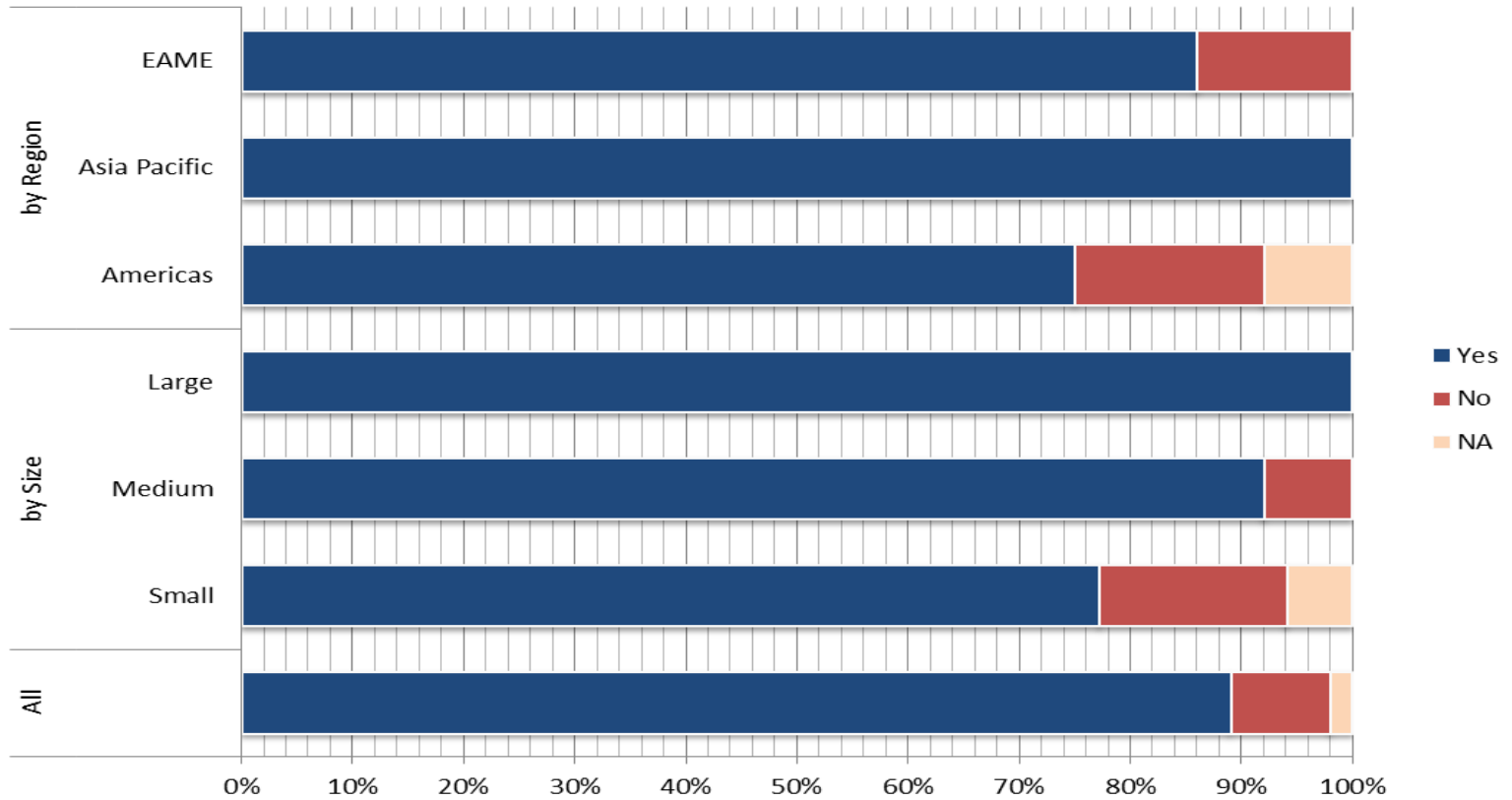
- Halting trading activity or affecting the ability of a clearing house to act as a central counter party within the settlement window
- Moving markets through takeover of accounts and unauthorized trading
- Targeting telecommunication networks supporting financial structures
- Ongoing data manipulation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

...exchanges exhibit a high-level of awareness and preparedness

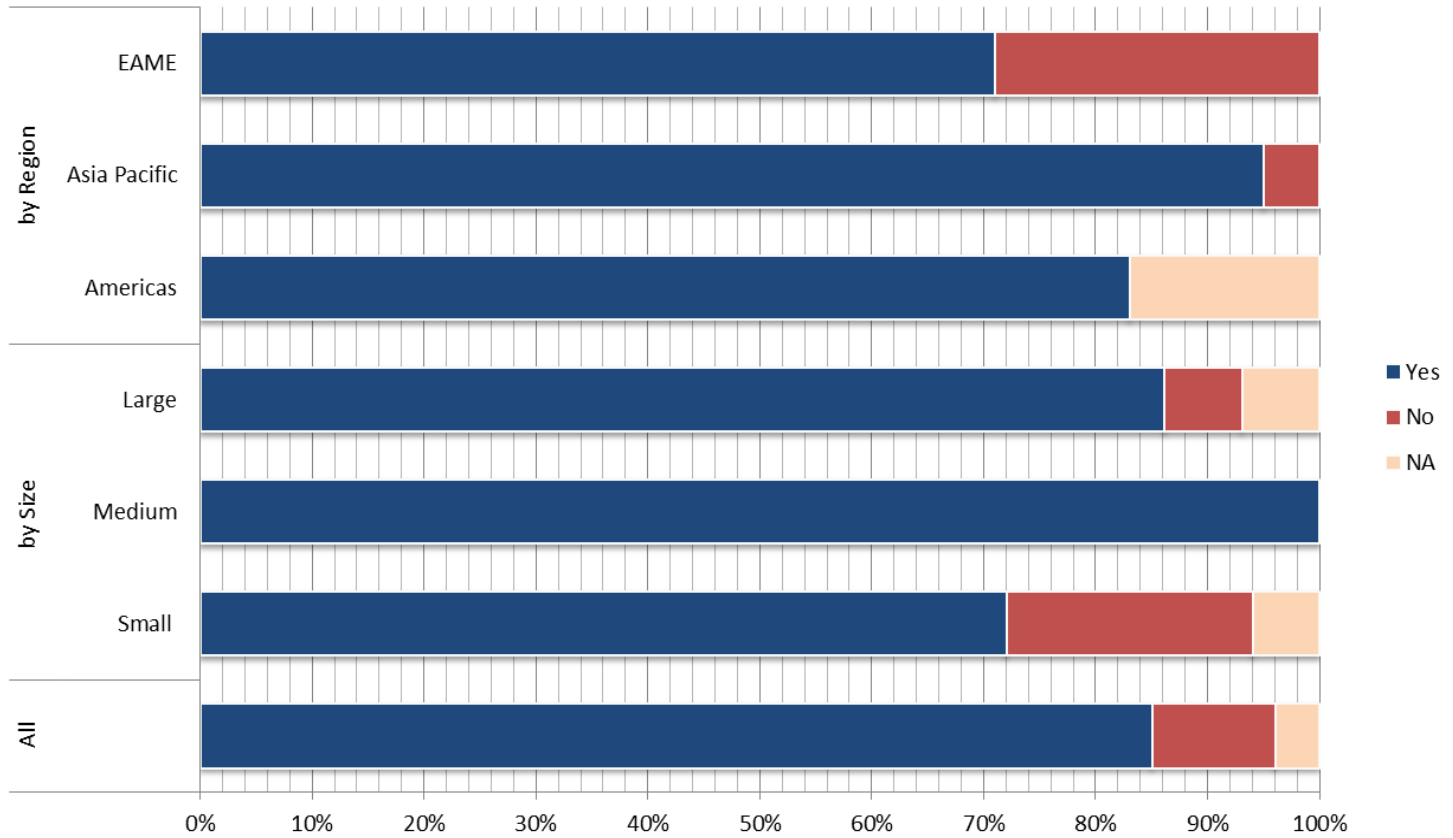
Discussed and understood by senior management?



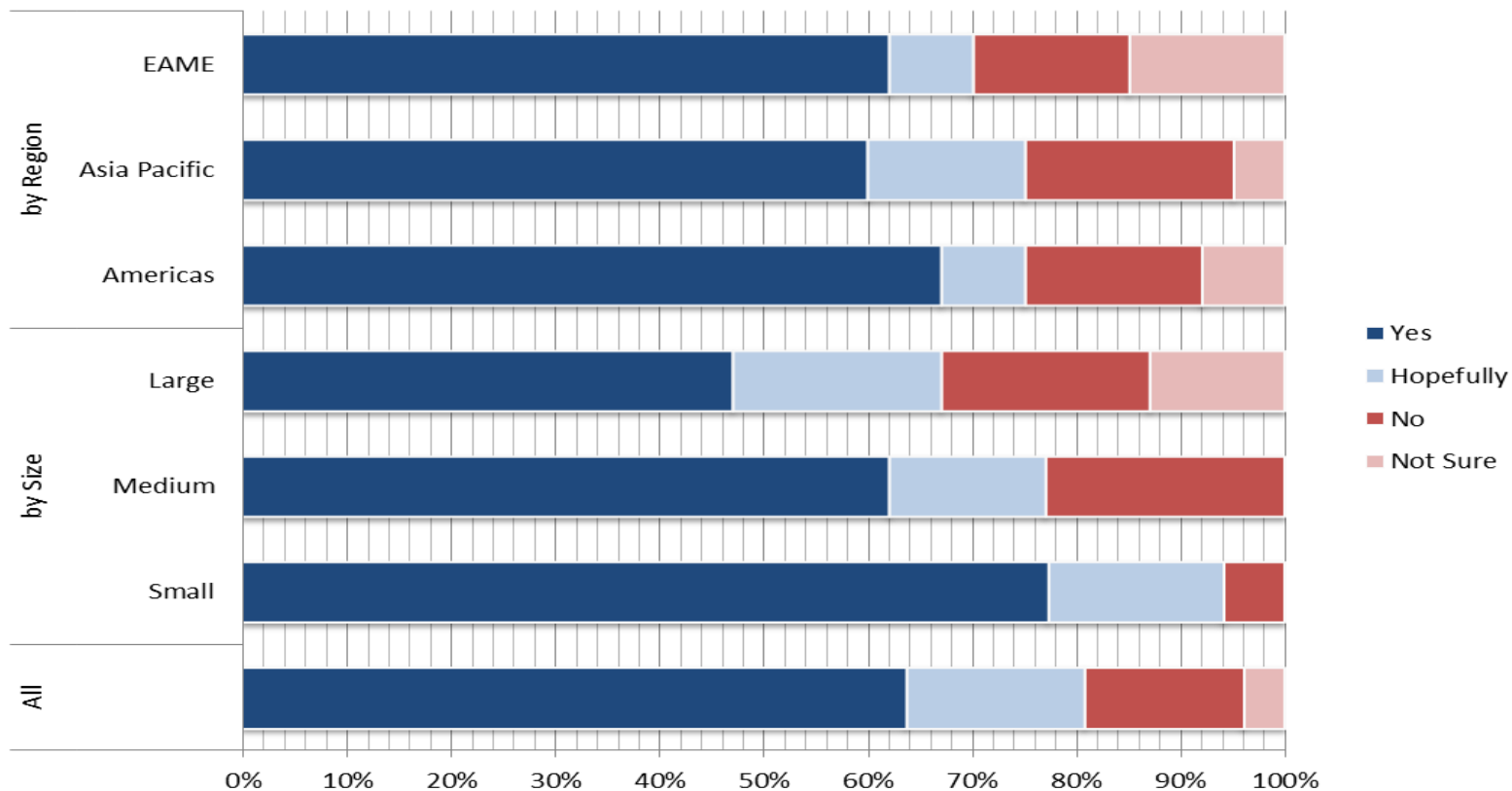
Formal plan for dealing with cyber-threats?



Staff training?

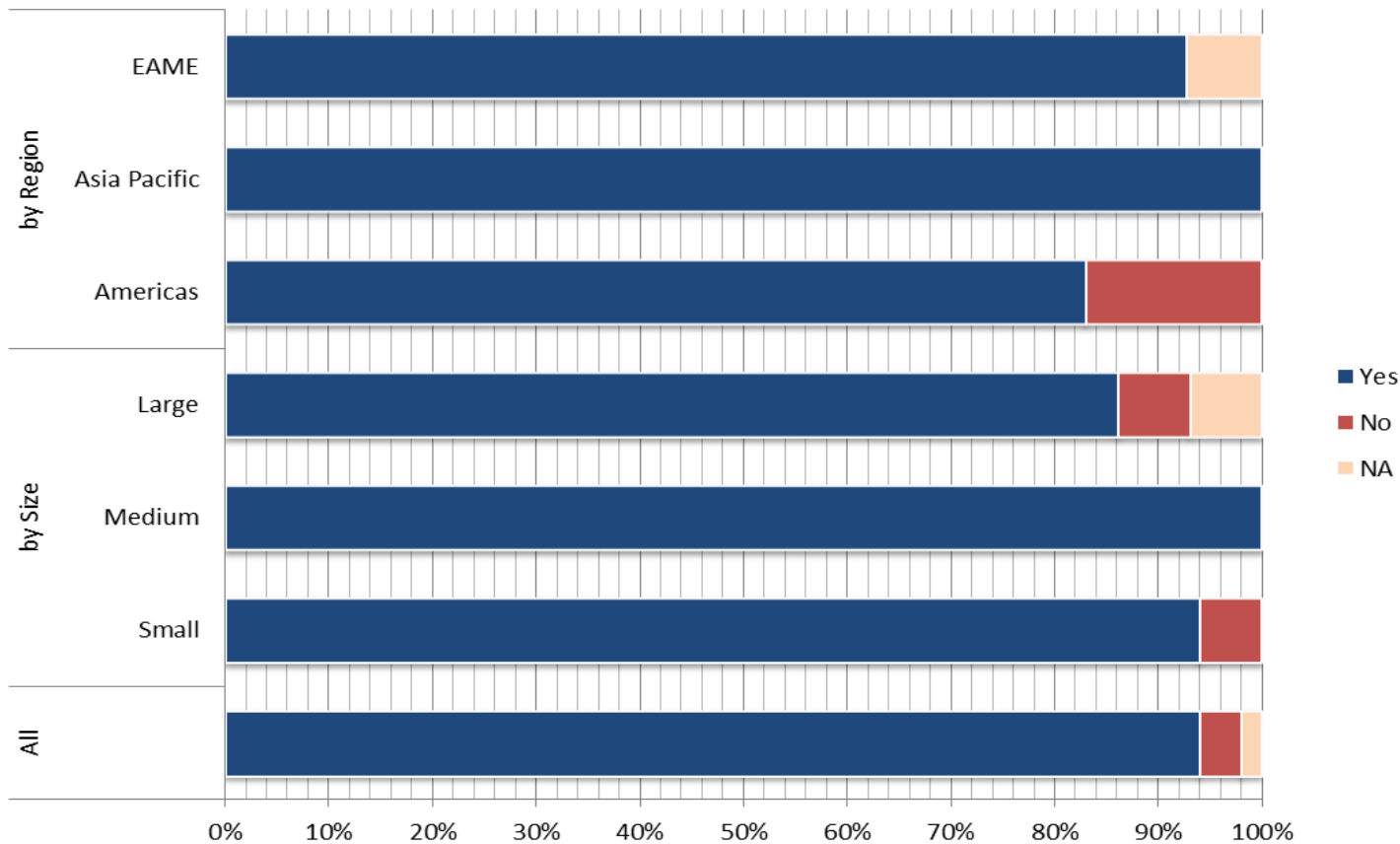


Preventative/detection measures sufficient?

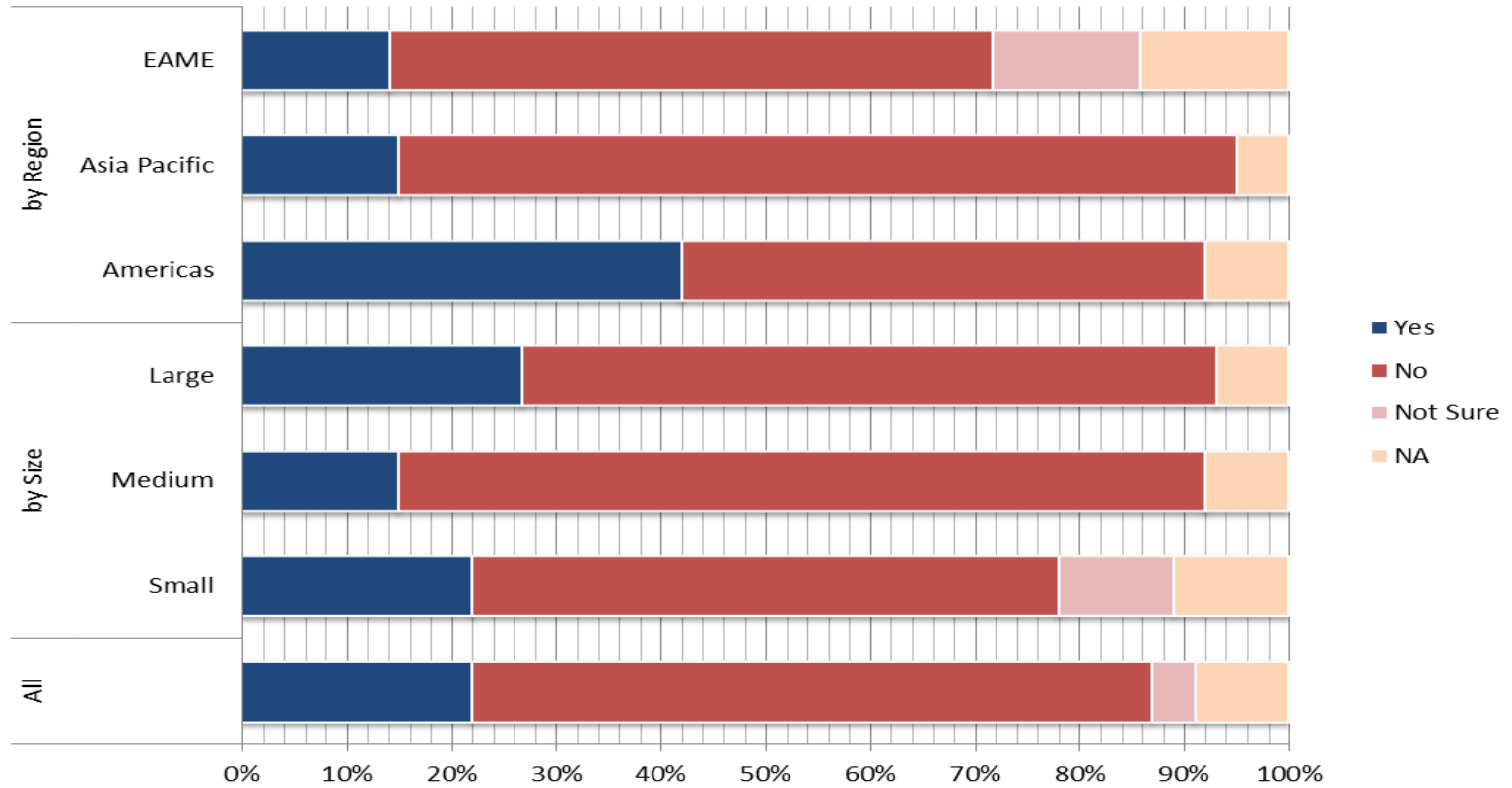


100% security is illusory yet...

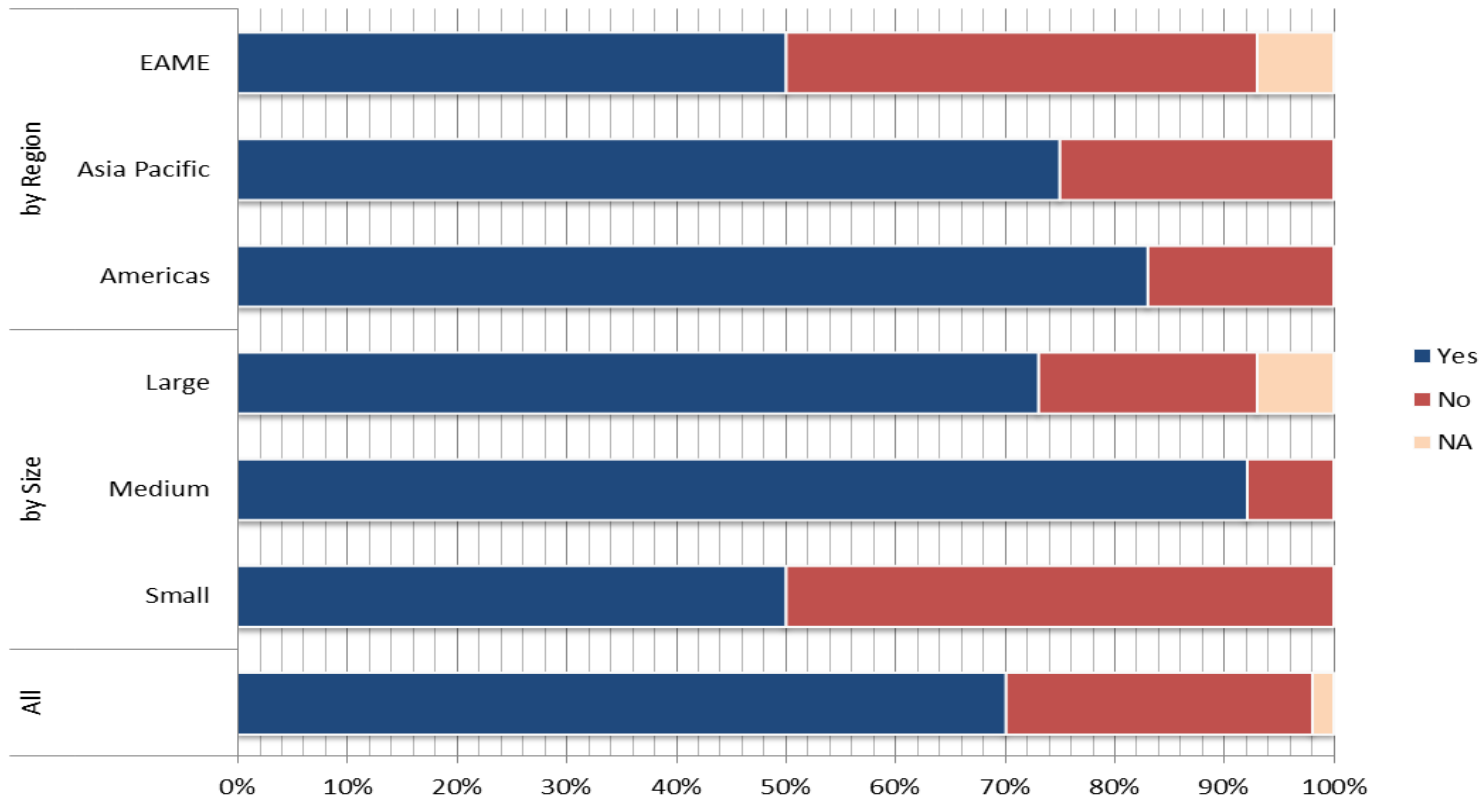
Disaster recovery measures?



Cyber-crime insurance?



Information sharing?

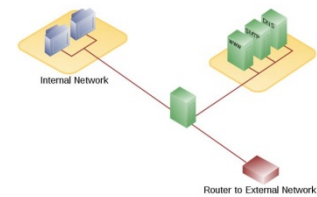


Content

- I. The cyber-threat to the financial system: tackling the myths
- II. Survey to the world's exchanges
- III. Measures and responses



≠



“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

See IOSCO/WFE report ‘Cyber-crime, Securities Markets and Systemic Risk’:

www.iosco.org/research

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