Government Security

Presented by Kumpol Sontanarat
Securities and Exchange Commission
May 14, 2014

IOSCO:Cyber-crime, securities markets and systemic risk

IOSCO (International Organization of Securities Commissions)
We has been an IOSCO ordinary member (with voting right) since 1992

Vast majority of respondents agree that cyber-crime in securities markets can be considered a potentially systemic risk (89%).

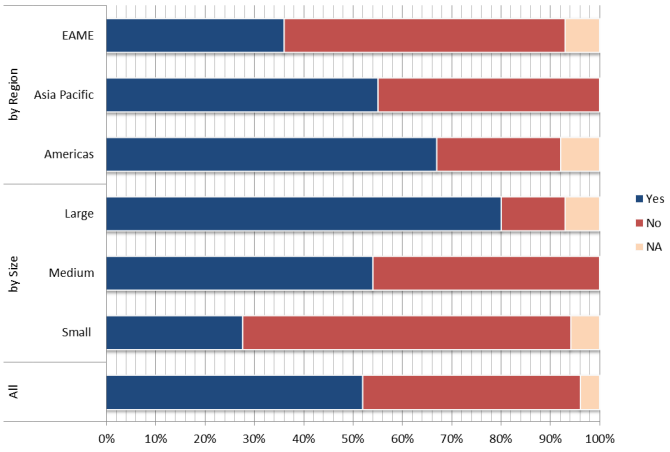
Theme 1: Size, complexity and incentive structure

-Over half of exchanges surveyed report experiencing a cyber-attack in the last year (53%)

- Attacks tend to be disruptive in nature (rather than aiming for immediate financial gain)

Theme 1: Size, complexity and incentive structure

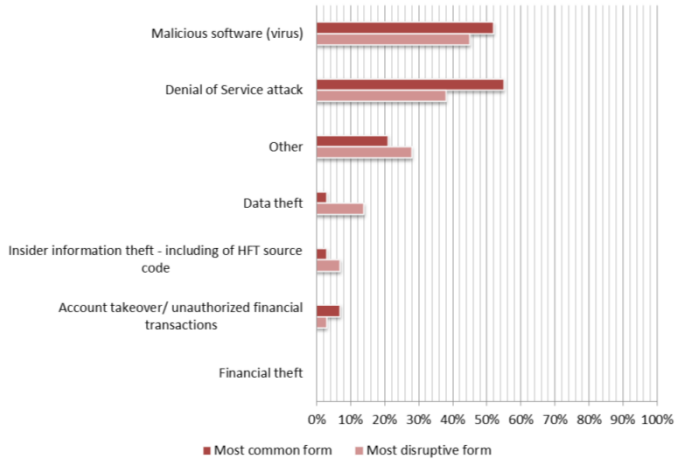
Exchanges from the Americas were more likely to report having suffered an attack (67%)



*The European-African-Middle Eastern (EAME)

Theme 1: Size, complexity and incentive structure

Attacks tend to be disruptive in nature (rather than aiming for immediate financial gain)

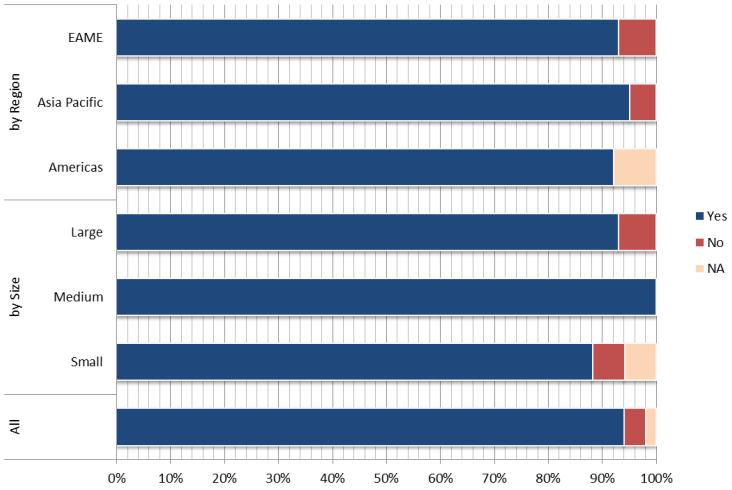


Theme 2: Market integrity, efficiency and infiltration of non-substitutable and/or interconnected services

Potentially aiming to choke essential financial services; steal/damage/manipulate information, money supply and markets; damage the capability of the private sector to ensure orderly functioning of the economy and delivery of services; and severely damage investor confidence.

Theme 3: Level of transparency and awareness

-Nearly all exchanges surveyed (93%) report that cyber-crime is generally understood and discussed by the senior management



Theme 4: Level of cyber-security and cyber-resilience

Cyber-security in exchanges generally engages with human vulnerabilities

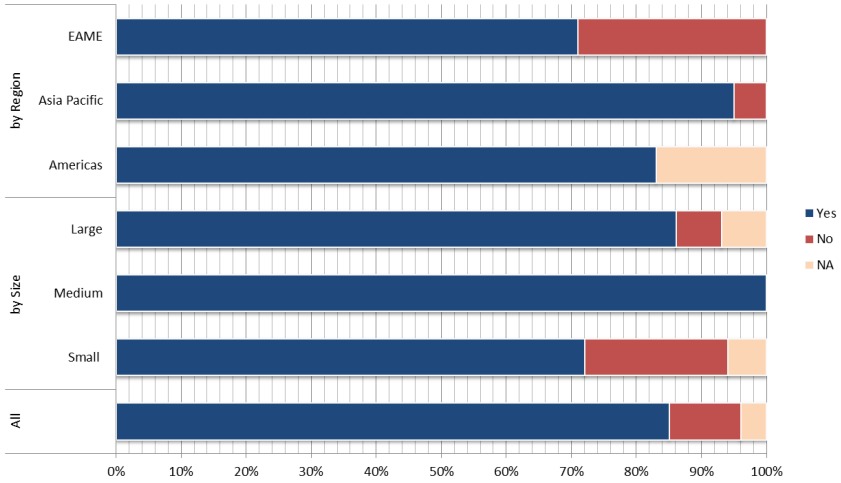
-85% of exchanges surveyed report that their organization undertakes cyber security related training for general staff

-however smaller exchanges were less likely to report providing it (72%).

-while the majority of respondents from the Asia Pacific region and Americas offer general staff training, almost 30% of respondents from the EAME region reported that they do not

Theme 4: Level of cyber-security and cyber-resilience

Example survey: Does your organization have cyber security related staff training for general staff?



Theme 4: Level of cyber-security and cyber-resilience

-Exchanges surveyed state that the most common and most disruptive cyber-attacks are generally detected immediately (within 48 hours).

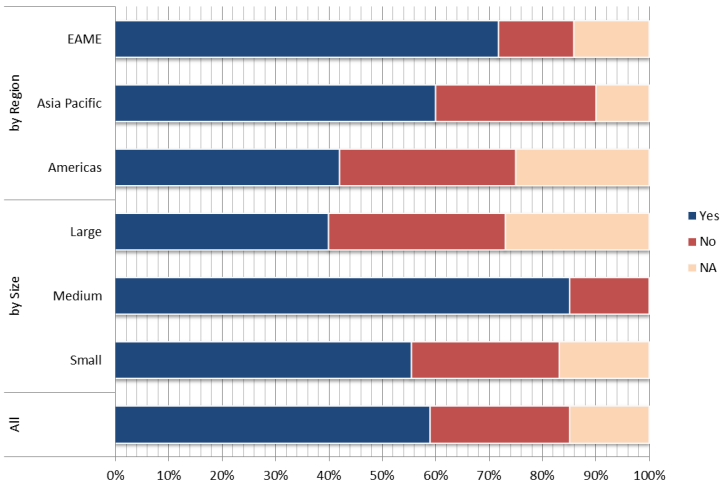
-The threat of long-term infiltration by ‘zero day’ threats can never be completely eliminated but can be mitigated through robust detection systems involving both internal and external, 24/7, monitoring and surveillance:

Theme 5: Effectiveness of existing regulation

Only 59% of exchanges surveyed report sanction regime being in place for cyber-crime, in their jurisdiction

Theme 5: Effectiveness of existing regulation

Are sanctions regimes in place?



Reference

http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf

END