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.
What is Cyber-Crime?

• Cyber-crime is a harmful activity executed through computers, IT systems and/or the internet and targeting the **confidentiality, integrity and accessibility** of computer systems, IT infrastructures and/or internet presence.

• It can include:
  – **traditional crimes** e.g. fraud, forgery executed over the internet;
  – publication of **harmful information** via electronic media;
  – **specifically internet-based crimes** e.g. denial of service, hacking;
  – and ‘**platform crimes**’ which use computer and information systems as a platform for performing other crimes e.g. use of botnets to control another user’s computer.
What is Cyber-Crime?

• Example 1:
The Stuxnet attack on Iran’s nuclear program, 2010. A sophisticated virus infiltrated the machine controlling gas centrifuges tasked with separating Uranium-235 isotopes from U-238 isotopes at the Natranz plant. As a result, the spin of the centrifuges were slowed, stalled and in some cases self-destructed. The perpetrator has still not been identified.

• Example 2:
The attack on South Korean banks and broadcasters, 2013. A suspected cyber-attack brought down systems and computers of some of South Korea’s major banks and broadcasters.
The evolving nature of cyber-crime

- **Increasing sophistication and complexity of cyber-crime**
  - Focus has shifted from systems (e.g. crashing systems) to information (e.g. manipulating/stealing information).
  - Attacks now utilize a variety of traditional cyber-crime techniques at once and utilize social engineering.
  - Attacks now specifically and strategically tailored for a particular entity rather than launched against as many users as possible. The more widespread the attack, the easier to detect and prevent it.
  - Rise of the Advanced Persistent Threat (APT): attacks mainly orchestrated for political or ideological aims rather than financial gain. They are generally very sophisticated and persistently employed over a number of years – they can go undetected for years.
Investigating Cyber-Crime in Securities Markets

- Limited study into cyber-crime in the world’s securities markets.

- Therefore, the IOSCO Research Department:
  - Jointly with the World Federation of Exchanges, sent a survey to the world’s exchanges on the topic.
  - Conducted market intelligence
  - Undertook a research and literature review
  - Member of CPSS-IOSCO working group on cyber-crime.

- The output of this work will be an exploratory research report.
The Survey

A survey designed by IOSCO Research Department and sent out by World Federation of Exchanges

- 23 quantitative and qualitative questions covering:
  - organizational approaches to cyber-crime;
  - statistics on cyber-attacks;
  - preventative and recovery measures;
  - information sharing;
  - the role of policy and regulation;
  - and insights into the systemic risk aspect of the threat.

- 75% response rate (46 responses in total)
Results: Preliminary assessment of the risk

- Securities markets, including systemically important institutions are already under attack and the threat is growing:
  - Over half (52%) of respondent exchanges to the WFE/IOSCO survey reported having experienced a cyber-attack in the last year.
  - In 2011, a PWC survey ranked cyber-crime as 2nd most commonly reported type of economic crime for financial sector organizations.
  - Cyber-crime has witnessed a dramatic rise since the beginning of the economic recession (an increase of 44% per year to an average of 1.4 attacks per week in 2011, per organization).
  - While a single cyber-attack against a critical or systemically important financial institution may not have systemic implications, a successful attack against 2, 3 or more institutions could have far-reaching consequences.
  - Some studies suggest that the cost of cyber-crime to society may be between $388 billion to $1 trillion so far.
Results: Preliminary assessment of the risk

- It’s cross-jurisdictional nature and current information-sharing arrangements may be contributing to a lack of transparency, obscuring the extent of the risk.
  - Survey reports that 70% of respondents is sharing information with the market, authorities, overseers or regulators however, most arrangements were national in nature.
  - Cyber-crime is perpetrated across nation state-borders.
  - The information required by authorities to investigate and understand the threat-landscape may be held outside an authorities’ jurisdiction.
Results: Preliminary assessment of the risk

- **Existing regulation may prove ineffective**
  - 59% of respondents reported sanction regimes being in place but only around half suggested they are currently effective.
  - International nature of these crimes makes it difficult to detect, prosecute and/or execute recuperative or responsive action.
  - Jurisdictional fragmentation; no global governance mechanism for cyber-crime related cases; legal and political barriers to overcome due to sovereignty, privacy and human rights.
  - Issue of attribution – difficult to pinpoint perpetrators as can wipe all traces.
  - A doctrine of deterrence may be ineffective since likelihood of being caught is low.
Conclusions & Ideas for Follow Up

Conclusions:

Cyber-crime:

• Threatens the orderly and efficient markets;
• Is a truly global problem;
• Is growing in size, sophistication, potential for disruption and destruction;
• And therefore a potential systemic risk.
Conclusions & Ideas for Follow Up

Questions for follow up:

• How can we intensify the identification of cyber crime?
• How can we better monitor?
• Would we need further research into indicators that can help identification, monitoring and measuring impact?
• How can we improve cross-jurisdictional/global information sharing and cooperation among industry, regulators and between them?
• Do we need global standards?