Cyber-crime, Securities Markets and Systemic Risk

Werner Bijkerk
Head of the Research Department

SROCC, Mid-Year Meeting
Toronto, 21 May 2013

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. What is cyber-crime? The nature of the threat
II. IOSCO Research Department's Research into Cyber-crime
III. Survey Results
IV. Can it be considered as a potential systemic risk?
V. Conclusions and ideas for follow up

Content

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

- **Expanding reach of cyber-crime**
  - As society and our securities markets rely increasingly on cyber-infrastructure, the potential reach of cyber-crime expands.
  - Currently most households and businesses are online and there is increasing use of social media for business purposes.

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.

The evolving nature of cyber-crime

- **Shifting motives, well-resourced actors**
  - Cyber-criminals are no longer only small-scale 'hackers' or hactivists interested in financial gain, notoriety or to push a particular message.
  - Can now be large, powerful and well-resourced groups with destructive, disruptive or potentially destabilizing political, economic or ideological aims
  - Actors can include: criminal groups; terrorists groups seeking to destabilize a government; political extremists who wish to damage the financial system; and a nation state wanting to attack an enemy state.
  - There is also a cyber-crime black market – where cyber-criminal skills and tools can be bought and sold.
- **Financial loss is therefore not the only cost to consider**
  - New types of cyber-criminals and more diverse motives means other consequences need to be considered – cyber-crime can also be perpetrated with the intention of disruption or destabilization.

Content

I. What is cyber-crime? The nature of the threat

II. IOSCO Research Department's Research into Cyber-crime

III. Survey Results

IV. Can it be considered as a potential systemic risk?

V. Conclusions and ideas for follow up

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**.*

Content

I. What is cyber-crime? The nature of the threat
II. IOSCO Research Department's Research into Cyber-crime
III. Survey Results
IV. Can it be considered as a potential systemic risk?
V. Conclusions and ideas for follow up

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: current state of play

- **Cyber-crime is increasingly being recognized as a core business issue and risk by most exchanges**
  - Almost all reported cyber-crime is generally understood and discussed by senior management of the world's exchanges.
  - 89% of respondents have a formal plan/documentation addressing cyber-attacks or cyber-threats.
  - Over two-thirds have an internal definition or use and existing definition of cyber-attacks or cyber-threats.
  - Clear upward reporting lines are present in the majority of exchanges.

Results: current state of play

- **Cyber-crime is being addressed at both the technical and 'human' level in most exchanges**
  - 85% of respondent organizations undertake cyber-security related training for general staff, smaller exchanges are less likely to provide it however.
  - For almost two thirds of respondents, training is repeated at least once a year.

Results: current state of play

- **Cyber-crime attacks against exchanges are detected relatively quickly, but there may be a gap in capturing new threats.**
  - Nearly all respondents noted that the most disruptive and destructive cyber-attacks are detected immediately.
  - 32% of respondents report that information security event monitoring includes external event monitoring via a vendor.
  - It was acknowledged that new, innovative attacks that follow 'unknown patterns' may result in longer detection periods in the future.
- **Resourcing of cyber-security may not be adequate**
  - Majority of respondents reported allocating less than 5% of their IT budget and less than 5% of full-time IT staff to information/cyber-security.

Results: current state of play

- **There is a gap in confidence when it comes to preventative measures and disaster recovery protocols employed.**
  - Exchanges employ a number of *preventative* measures, including proactive defenses such as risk registers and scenario planning.
  - However, only 63% of respondents are confident that preventative measures are currently employed successfully in their organization – Respondents from larger exchanges were most likely to think otherwise.
  - Furthermore, while 94% of respondents report disaster recovery protocols in place, only 60% are confident that they are sufficient in their current form.
  - Only 22% of respondents have cyber-crime insurance or something similar. Most responses mentioned that insurance was: not available, cost-prohibitive, have significant coverage limitations (e.g. reputational damage not considered) or that it is under consideration.

Results: current state of play

- **There may be limited engagement with cyber-physical threats**
  - Less than half of respondents report utilizing a merged group to handle both information security and physical security threats.
  - There are some clear overlaps between the physical and cyber world.
  - In some cases cyber-attacks can be perpetrated to distract from an impending physical attack, or vice versa.

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

- **Cyber-crime could undermine market integrity and efficiency, and confidence in the system:**
  - Survey reported a high correlation between most disruptive attacks and the most common form of cyber-attack experienced (i.e. Denial of Service attacks and malicious software (viruses)).
  - Disruptive attacks on large players could disrupt critical functioning of the market and impact confidence in the financial system - halting activity completely.
  - Numerous attacks on smaller players (including investors) could also impact confidence in the financial system. For example, loss of confidentiality of data due to a breach in a number of smaller firms or unauthorised leakage of information could erode investor confidence in capital markets in the longer-term.

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.

Content

I. What is cyber-crime? The nature of the threat
II. IOSCO Research Department's Research into Cyber-crime
III. Survey Results
IV. Can it be considered as a potential systemic risk?
V. Conclusions and ideas for follow up

Cyber-crime and systemic risk

"a risk of disruption to financial services that (1) is caused by an impairment of all or parts of the financial system and (2) has the potential to have serious negative consequences for the real economy."

- The majority (89%) of respondents to the WFE/IOSCO survey agree that cyber-crime should be considered a potential systemic risk.

Cyber-crime and systemic risk

- Most affirmative responses point to the possibility of:
  - massive financial and reputational impact;
  - loss of confidence;
  - affect on market availability and integrity;
  - the interconnectedness and dependencies in securities markets;
  - and related knock-on effects on market participants from an attack.

- For some experts, a successful large-scale attack on the financial system could have catastrophic consequences for the economy.

Cyber-crime and systemic risk

Impact factors to determine whether risks of cyber crime can be systemic:

- Size:
  - Trends in frequency of attacks, number of targets.
  - Cost of attacks
- Cross-jurisdictional
- Interconnectedness and concentration:
  - Intra-financial system dependencies
  - Network concentration
- Substitutability:
  - Single-dependency on financial systems/entities (locked-in)

Cyber-crime and systemic risk

Impact factors (continued):

- Transparency/Opacity
  - Awareness of the threat at all levels.
  - Information sharing arrangements to understand and appropriately engage with the threat.
- Market integrity and efficiency
  - Number of complete disruptions/disorder of crucial financial services
  - Investor confidence in stability of systems
- Behaviour and incentive structure
  - Criminal: theft and money gains
  - Terrorist: destruction and disruption
  - Political “Cold war”: espionage, disruption

Cyber-crime and systemic risk

Impact factors (continued):

- Regulation
  - No global standards.
  - Jurisdictional conflicts/ambiguity.
  - Possibilities for regulatory arbitrage.
  - Deterrence and enforcement.
- Complexity
  - Sophistication of techniques.
  - Utilizing social engineering.
  - Executed over a long period, without detection.

Content

I. What is cyber-crime? The nature of the threat
II. IOSCO Research Department's Research into Cyber-crime
III. Survey Results
IV. Can it be considered as a potential systemic risk?
V. Conclusions and ideas for follow up

Conclusions & Ideas for Follow Up

Conclusions:

Cyber-crime:

- Threathens 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

Ideas for follow up:

- Intensification of identification;
- Closely monitoring;
- Further research into indicators that can help identification, monitoring and measuring impact;
- Cross-jurisdictional/global information sharing and cooperation among industry, regulators and between them;
- Discussion on the need for global standards.