OICV-IOSCO

Cyber-crime, securities markets and systemic risk

16 July, 2013

Joint Staff Working Paper of the IOSCO Research Department and World Federation of Exchanges

Author: Rohini Tendulkar (IOSCO Research Department)

Survey: Grégoire Naacke (World Federation of Exchanges Office) and Rohini Tendulkar

For further information please contact: research@iosco.org

Contents

About this Document

The IOSCO Research Department produces research and analysis around IOSCO Principle's 6 (*on systemic risk*) and 7 (*reviewing the perimeter of regulation*). To support these efforts, the IOSCO Research Department undertakes a number of annual information mining exercises including extensive market intelligence in financial centres; risk roundtables with prominent members of industry and regulators; data gathering and analysis; the construction of quantitative risk indicators; a survey on emerging risks to regulators, academics and market participants; and review of the current literature on risks by experts.

This holistic approach to risk identification is important in capturing those potential risks that may not be apparent in the available data (i.e. not necessarily quantifiable), or which may be currently seen as outside the perimeter of securities market regulation – but nonetheless relevant.

One potential risk that has been strongly and consistently highlighted during recent risk identification activities (and in the 2012 IOSCO Securities Market Risk Outlook) is **cyber-crime**, especially as it relates to financial market infrastructures. As a first step towards engaging with this issue, the IOSCO Research Department, jointly with the World Federation of Exchanges, conducted a *cyber-crime survey* of the world's exchanges.

This IOSCO Staff Working Paper *Cyber-crime, Securities Market and Systemic Risk* presents the results of this survey, as well as key insights on the current cyber-threat landscape and potential systemic risk aspects.

This report and survey is intended as part of a series exploring perspectives and experiences with cyber-crime across different groups of securities market actors. The purpose of the series is predominantly to: (1) deepen understanding around the extent of the cyber-crime threat in securities markets; (2) highlight potential systemic risk concerns that could be considered by securities market regulators and market participants; and (3) capture and synthesize into one document some of the key issues in terms of cyber-crime and securities markets in order to increase general understanding and awareness.

Executive Summary

Introduction

- The soundness, efficiency and stability of securities markets relies on the quality of information provided; the integrity of people and service provision; the effectiveness of regulation; and increasingly the robustness of supporting technological infrastructure. Yet, there is limited public, targeted and in-depth study into how one of the more prominent technology-based risks: cyber-crime could and is impacting securities markets.
- Cyber-crime can be understood as an attack on the confidentiality, integrity and accessibility of an entity's online/computer presence or networks – and information contained within.

The Evolving Nature of Cyber-Crime

- In recent years, cyber-crime has become increasingly sophisticated, making it difficult to combat, detect and mitigate. The rise of a relatively new class of cyber-attack is especially troubling. This new class is referred to as an 'Advanced Persistent Threat' (APT).[1]
- The costs of cyber-crime to society so far may already be substantial. Some studies cite figures as high as $388 billion[2] or $ 1 trillion[3]. While these high numbers are contentious due to lack of reliability when it comes to reporting direct and indirect costs, a growing number of high-profile cyber-attacks, high financial losses incurred, and other real-world manifestations suggest a potential for widespread impact.

A focus on the world's exchanges

- To gather unique insights into the cyber-crime threat from a securities market perspective, the IOSCO Research Department, jointly with the World Federation of Exchanges Office, conducted a cyber-crime survey (*hereafter the WFE/IOSCO survey*) to some of our core financial market infrastructures - the world's exchanges.[4]
- This survey is intended as part of a series of surveys exploring perspectives and experiences with cyber-crime across different groups of securities market actors, financial institutions and regulators.
- In this first survey, a vast majority of respondents agree that cyber-crime in securities markets can be considered a potentially systemic risk (89%). The following factors shed light on why:
- **Size, complexity and incentive structure**
  - Cyber-crime is already targeting a number of exchanges. 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). The most common forms of attack reported in the survey are Denial of Service attacks and malicious code (viruses). These categories of attack were also reported as the most disruptive. Financial theft did not feature in any of the responses.

[1] Advanced Persistent Threats (APTs) are usually directed at business and political targets for political ends. APTs involve stealth to persistently infiltrate a system over a long period of time, without the system displaying any unusual symptoms.
[2] Norton, Cybercrime Report, 2011
[3] The Global Industry Analysts; McAfee, 'Unsecured Economies: Protecting vital information' 2011
[4] 75% of exchanges contacted, responded to the survey (in total 46 exchanges).

- This suggests a shift in motive for cyber-crime in securities markets, away from financial gain and towards more destabilizing aims. It also distinguishes cyber-crime in securities markets from traditional crimes against the financial sector e.g. fraud, theft.

- **Potential effect on market integrity and efficiency; infiltration of non-substitutable and/or interconnected services**
  - The instances of attacks against exchanges means that cyber-crime is already targeting securities markets' core infrastructures and providers of essential (and non-substitutable services). At this stage, these cyber-attacks have not impacted core systems or market integrity and efficiency. However, some exchanges surveyed suggest that a large-scale, successful attack may have the potential to do so.
- **Level of transparency and awareness**
  - Transparency in the form of information sharing is occurring widely. 70% of exchanges surveyed note that they share information with authorities, overseers or regulators. However, most of these arrangements are national in nature.
  - There is also a high level of awareness of the threat across exchanges surveyed. Around 93% of exchanges surveyed report that cyber-threats are discussed and understood by senior management and almost 90% report having in place internal plans and documentation addressing cyber-crime.
- **Level of cyber-security and cyber-resilience**
  - All exchanges surveyed appear to have in place myriad proactive and reactive defence and preventative measures (see Annex B) and report that cyber-attacks are generally detected immediately. Annual cyber-crime training for general (non-IT) staff is also a staple amongst the majority of respondent exchanges.
  - However, a small but significant number of exchanges surveyed recognize that 100% security is illusionary, with around a quarter recognizing that current preventative and disaster recovery measures may not be able to stand up against a large-scale and coordinated attack.
  - Around half of exchanges surveyed report having two separate groups for handling physical and cyber threats. Separation of the two teams could lead to challenges in engaging with cyber-physical threats, however these challenges may be easily overcome (if not already) through efficient and on-going coordination between the two groups. Further information around the level of coordination between these two groups could shed light on this point.
  - Around 22% of exchanges surveyed report having cyber-crime insurance or something similar. This is mainly due to lack of availability or insufficient coverage of available insurance.
- **Effectiveness of regulation**
  - A number of respondents expressed doubt over the effectiveness of current regulation in deterring cyber-criminals from damaging markets, since the global nature of the crime makes it difficult to identify and prosecute them. Only 59% of exchanges surveyed report sanctions regimes being in place for cyber-crime, in their jurisdiction. Of these, only half (55%) suggest that current sanction regimes are effective in deterring cyber-criminals.

Engaging with the risk

- In terms of the future role of securities market regulators in engaging with cyber-crime in securities markets, the following activities were highlighted most frequently by exchanges surveyed:
  - Updating/implementing regulation and standards (in collaboration with other authorities);
  - Identifying and providing guidance on best practice, principles and/or frameworks;
  - Building, partaking in and promoting information sharing networks;
  - Acting as a repository of knowledge for securities market participants to tap into (e.g. keep up to date with trends, house technical expertise to answer industry questions, collect and record cases, identify biggest risks).
- Many of the exchanges surveyed underline a need for further policy but assert that any efforts in this space should:
  - avoid being prescriptive;
  - maintain flexibility to adapt to changing risks;
  - concentrate on information sharing; effective regulations/legislation; providing guidance and principles; and not interfere with an institution's own tailored internal measures or policy.

Introduction

"Thousands of cyber-attacks […] are striking at the private sector, strike at Silicon Valley, strike at other institutions within our society, strike at government, strike at the defence department, our intelligence agencies. Cyber is now at a point where the technology is there to cripple a country, to take down our power grid systems, to take down our government systems, take down our financial systems and literally paralyze the country."

Leon Panetta, former U.S. Secretary of Defence

As part of the objectives of IOSCO, securities market regulators agree to encourage and maintain the soundness, efficiency and stability of markets and address systemic risk. This is achieved at the global level through cooperative tools such as (1) the IOSCO Multilateral Memorandum of Understanding (MMoU), a global information sharing agreement between securities regulators; (2) IOSCO's Objectives and Principles of Securities Regulation; (3) and the CPSS/IOSCO Principles for Financial Market Infrastructures (PFMIs). Today, the soundness, efficiency and stability of securities markets relies not only on the quality of information provision; the integrity of people and service provision; and the effectiveness of regulation[5] - but increasingly on the robustness of supporting technological infrastructure. This makes cyber-based attacks on securities markets' technological infrastructure an area requiring further investigation from a securities market perspective and as a potential systemic risk.

What is cyber-crime?

Cyber-crime is most commonly understood as involving an attack on the confidentiality, integrity and accessibility[6] of an entity's online/computer presence or networks. The IOSCO Research Department tentatively defines 'Cyber-Crime' as: a harmful activity, executed by one group (including both grassroots groups or nationally coordinated groups) through computers, IT systems and/or the internet and targeting the computers, IT infrastructure and internet presence of another entity. An instance of cyber-crime can be referred to as a cyber-attack.[7]

There is some contention and ambiguity around exactly what activities fall under the classification of cyber-crime, however generally cyber-crime can be categorized as follows:[8]

- Traditional crimes e.g. fraud, forgery, which are now committed via electronic networks and information systems;
- Publication of harmful, illegal or false information via electronic media;
- New crimes that have emerged due to the unique opportunities presented by the internet 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.[9]

[5] Bernard Black, "The Core Institutions that Support Strong Securities Markets", *The Business Lawyer*, Vol. 55, No 4, August 2000
[6] Known as the CIA triad.
[7] A single cyber-attack can refer to an individual hit against an organization or a grouping of multiple hits against an organization.
[8] List from European Commission, 'Towards a general policy on the fight against cyber-crime', Communication, May 2007; and Ross Anderson, Chris Barton, Rainer Bohne, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore, Stefan Savage "Measuring the Cost of Cybercrime", 2012
[9] A botnet essentially gains controls of multiple computers and can order them to perform certain tasks remotely e.g. send spam, without the actual users being aware of it.

For the purposes of this report, cyber-crime can also involve data theft, destruction or manipulation; identity theft; monetary theft; disruption of IT services; and in some cases - cyber-espionage and cyber-terrorism.[10] Box 1 presents a list of recent and prominent cyber-attacks on different sectors, revealing the potential for real-world impacts.

Box 1: Examples of cyber-attacks

- *Attack on South Korea's banks and broadcasters, 2013.* A suspected cyber-attack brought down systems and computers at some of South Korea's major banks and broadcasters. As a result, the local equity market declined 1.0%.
- *Operation High Roller.* Orchestrated in 2012 the attack siphoned around $78 to $2.5 billion from bank accounts in Europe, the U.S. and Latin America. Targets were high-value commercial accounts, rich individuals, credit unions and large global banks and regional banks. The attack located a victim's highest value account and transferred money to a prepaid debit card (which can be cashed in anonymously). The target's bank statement was then altered to hide the theft.[11]
- *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.
- *Cyber-attack against state-owned oil company Aramco.* Over 30 000 computers at Saudi Arabian oil company Aramco were hit by a devastating virus in August 2012. The attack destroyed data and erased hard-drives of computers and is thought to have been aimed at stopping the production of oil.
- *The Flame virus, 2012.* Thought to have been operating since 2010, the Flame virus was detected in 2012. The virus code is seen as some of the most sophisticated and largest malicious code to date. It infiltrated computers belonging to the Iranian Oil Ministry, the Iranian National Oil Company and other networks in Hungary, Lebanon, Austria, Russia, Hong Kong and the United Arab Emirates - stealing and deleting information from the systems. Part of the functionality of the virus including turning on microphones of computers to secretly record conversations, taking screen grabs of infected computers and stealing credentials of high-level and administrative users.
- *Red October cyber-attack*, 2013. Targeting governmental and diplomatic organisations. The Red October attack was discovered in January of this year, but is believed to have been operating undetected for a number of years. The attack effectively stole confidential and encrypted documents (including deleted ones) from embassies, nuclear research centres and oil and gas companies. Information targeted included geopolitically sensitive data and credentials to access protected computer systems. The malicious code was also able to detect when a USB stick was inserted into a networked computer and undelete and steal any files on the stick.[12] The cyber-crime racket behind the attacks shut-down their operations after the attacks were made public and documented.
- *The MiniDuke Cyber-attack on EU governmental organizations and operators of critical infrastructure*.[13] The MiniDuke Cyber-attack exploited a flaw in Adobe's Acrobat reader to enter computer networks and gather information.
- *Attack on U.S. natural gas pipeline.* A report from the U.S. Department of Homeland Security (DHS) suggests

[10] Cyber-terrorism is defined as ""the use of computing resources against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives" in *Cybercrimes: Infrastructure Threats from Cyberterrorists*, Cyberspace Lawyer, Cyberspace Law, 4, No. 2

[11] See Reuters, Joseph Menn, 'New Bank theft software hits three continents: researchers', June 26 2012 and Business Insider, Michael Kelly, 'Operation High Roller', Jun 28 2012.

[12] BBC, Dave Lee, 'Red October' cyber-attack found by Russian researchers', 14 January 2013.

[13] ENISA, Flash Note, *Cyber-attacks – a new edge for old weapons*, 13 March 2013.

an increase of attacks on critical infrastructure. Out of 198 attacks reported to the DHS, 82 attacks were against the energy sector and 29 attacks were against the water industry. Chemical plants faced seven attacks and nuclear companies faced 6. In one instance, an unidentified hacking group stole information which could allow them to remotely infiltrate the control systems of a natural gas pipeline, although the system itself was not compromised.[14]

- *First documented attack on a U.S. election, 2012.* A grand jury report[15] on the primary elections in Florida, U.S., in 2012, identified a cyber-attack against the electronic election system, where around 2500 fraudulent requests for absentee ballots were lodged. Most of the computers involved in the attack had overseas IP addresses.
- *Operation Aurora, 2009.* Attacks against some of the largest internet, technology and defence companies such as Google, Adobe, Juniper, Yahoo!, Northrup Grumman. The cyber-attack modified source code by exploiting vulnerabilities in an internet browser.
- *Cyber-attacks on media – censoring the press, 2012.* A recent spate of cyber-attacks targeting content on high-profile media outlets such as the New York Times, Wall Street Journal and Washington Post and social networking sites such as Twitter. Traditional anti-virus software and firewall proved ineffective in these attacks. The growth of 'mobile applications' is also providing entry for would-be hackers.

Awareness of the cyber-crime risk in securities markets

Awareness of cyber-based risks in different sectors is gradually increasing and has already been at least partially addressed in some regulations around the world,[16] taken up through practical industry-wide initiatives[17] and captured in a number of reports and surveys.[18] World leaders, experts and prominent figures have also openly acknowledged the cyber-threat to society and the economy[19] and Governments are actively and transparently elevating cyber-

[14] U.S. Department of Homeland Security, ICS-CERT Monitor, October/November/December 2012 [http://ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf]

[15] 'Financial Report of the Miami-Dade County Grand Jury', in the circuit court of the Eleventh Judicial Circuit of Florida in and for the County of Miami-Dade, Spring Term A.D. 2012. [http://www.miamisao.com/publications/grand_jury/2000s/gj2012s.pdf]

[16] **U.S.:** In 2009, The Obama Administration put forward Cyber security policy. While the proposed Cyber security Act has not passed the Senate, numerous agencies have been set up to fight cybercrime e.g. in the FBI, National Infrastructure Protection Centre, Internet Fraud Complaint Centre, Computer Crime and Intellectual Property and Computer Hacking and Intellectual Property Units (Department of Justice), Computer Emergency Readiness Team/Coordination Centre (CERT/CC). On the financial sector side specifically, the U.S. SEC provided cyber-security guidelines in October 2011 and mandated that publicly registered companies disclose if they have suffered a 'reasonably serious' attack. **China:** has put in place a number of rules concerning cyber-crime, since 2000. China has also signed the UN General Assembly Resolution (57/239) on cyber security and the Geneva Declaration of Principles of the World Summit of Information Society. China has also initiated the 'Golden Shield Project' and 'The Great Firewall of China to control internet use. **Europe:** The European Commission has a number of digital security policies in place. The Council of Europe also proposed a Cyber-crime convention. The European Union recently proposed new regulations calling for creating of Computer Emergency Response Teams in each jurisdiction and the establishment of a body responsible for processing security breach reports. The regulations also propose that authorities should have discretion around publicising attacks and fining companies for lax security measures. The European Council. In the UK the Financial Services Authority ("FSA") has included "Data Security" within its top economic crime risks. **Other Jurisdictions: [**See cybercrimelaw.net]

[17] For Example the European Joint Research Centre and SIFMA have coordinated wide-scale 'on the ground' training and simulations for firms, working through a number of cyber-attack scenarios in order to promote awareness and skills.

[18] For example: Norton, '2012 Norton Cybercrime Report', [http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport]; RSA, 2012 Cybercrime Trends Report.

[19] A number of prominent figures and experts have highlighted the increasing scale of the cyber- threat and potential for systemic consequences, as well as the urgency faced – invoking expressions such as 'Cyber Pearl Harbour' or '9/11 type event': *"It's a big deal; it's going to get worse",* Jamie Dimon, CEO of JP Morgan at Panel Discussion, Council of Foreign Relations 10 October 2012*; "All of a sudden, the power doesn't work, there's no way you can get money, you can't get out of town, you can't get online, and banking, as a function to make the world work, starts to not be reliable…Now, that is a cyber-Pearl Harbor, and it is achievable.",* John McConnel, director of the National Security Agency under President Clinton, director of national intelligence under George W. Bush and President Obama*; "I think that it is near-term…. I'm quite frankly surprised it hasn't happened yet"* Shawn Henry, FBI cyber unit; *"… nearly everyone in the business believes that we are living in, yes, a pre-9/11 era when it comes to the security and resilience of electronic information systems. Something very big… is likely to go wrong, they said, and once it does, everyone will ask how we could have been so complacent for so long."* James Fallows, journalist in 'Cyber Warriors', The Atlantic, 1 March 2010

related risks into a national security issue.[20] Cyber-based threats are also being recognized more generally as constituting a top economic risk. In a 2012 World Economic Forum risk report, cyber-attacks ranked as 4th most likely risk faced, and in the 2013 edition cyber-attacks, data fraud/theft and digital misinformation were noted as possible contributors to 'digital wildfires in a hyper connected world'.[21]

Furthermore, the potential reach of cyber-crime is vast - including much of our economy. For example: 70 per cent of households and 94 per cent of businesses with 10 or more employees are online;[22] there is exponential growth of internet-connected mobile devices;[23] social media is now used profusely for both personal and business pursuits; many businesses are turning to cloud computing to store data, due to cost efficiencies[24]; and banking and other financial services providers all rely on technology of some kind to disseminate information and execute business rapidly.[25] The World Economic Forum notes *"The scale and speed of information creation and transfer in today's hyper connected world [is]… historically unparalleled."*[26]

However, in the financial sector, views on the potential severity of cyber-attacks are mixed. On one hand, a number of prominent figures and experts highlight the increasing scale of the risks posed by cyber-crime in the financial sector, and the urgency faced – warning of an impending '9/11 type event'. In fact, the U.S. House Intelligence Committee suggested that it could be a successful and large-scale attack on financial institutions that brings about the 'doomsday' scenario or 'cyber-crisis' many fear.[27]

Others question whether cyber-crime in the financial system is a substantial risk, pointing out the actors most likely able to execute a cyber-attack of significant magnitude (i.e. nation states) have a stake in keeping the global financial systems stable – relying on the idea of mutually assured destruction.[28] However, there are important distinctions between physical and cyber threats to consider which may mean that the idea of mutually assured destruction may not hold. The build-up of cyber-crime capabilities can be more easily hidden than the build-up of physical offensive capabilities. Also, a physical threat has an immediate, observable outcome and is relatively easy to trace – while a cyber-threat may not be. It can take many years before the victim is aware they are even under attack and several more before they can identify the perpetrator and the full extent of the damage.

Regardless, contrasting views on the dangers posed by cyber-crime to the financial system may stem from confusing terminology, ambiguous definitions, and sometimes exaggerated language.[29] This uncertainty or disagreement around the nature and potential impacts of cyber-crime could result in an inappropriate response to the threat. A report on risks by the World Economic Form warns not only of "the challenge presented by the misuse of an open

[20] In the U.S., President Barack Obama established a Cyber Command (Cybercom) and in the UK, a cyber-security policy 'operations centre' has been set up in GCHQ.
[21] World Economic Forum, 2013, 'Insight Report: Global Risks 2013', 8th edition.
[22] Resilience in the Cyber Era: Building an Infrastructure that secures and protects, Economist Intelligence Unit and Booz Allen Hamilton, 2011
[23] Booz Allen, top ten cyber security trends for financial services in 2012, 2011
[24] Ernst & Young, Global Information Security Survey, 2011
[25] PWC, "Fighting Economic Crime in the Financial Services Sector", Survey, 2012
[26] World Economic Forum, 2013, 'Insight Report: Global Risks 2013', 8th edition
[27] In CNN Politics, 'Cyberthreats getting worse, House intelligence officials warn', 17 March 2013
[28] Panel: The Future of Conflict Panel at RSA, San Francisco
[29] Peter Sommer, Ian Brown, 'Reducing Systemic Cybersecurity Risk', OECD/IFP Project on 'Future Global shocks', *OECD,* 2011

and easily accessible [digital] system" but also "the greater danger of misguided attempts to prevent such outcomes".[30] Thus, research into the nature of the threat and what aspects may pose a systemic risk, is vital.

There has already been broad research conducted into technology-based threats, including to the financial sector, but there is limited public, targeted and in-depth study into how cyber-crime could and is impacting the world's securities markets. This research report engages with this gap, through exploring the cyber-crime risk in securities markets from a systemic risk perspective: highlighting the evolving nature of cyber-crime, the state of play when it comes to the protection of some of our core infrastructure, and general issues to consider by both regulators and market participants, going forward.

Such an investigation is especially salient given the financial crisis of 2007, its continuing and devastating after-effects and the increasing role of securities markets as a financing channel around the world. The crisis is also a strong reminder that even those (perceived) 'lower-probability, high impact' risks, should be considered and mitigated if the road towards financial resilience is to be paved. There is an added urgency in addressing these risks given that the financial system is still struggling towards recovery, and public trust and confidence in the system may be fragile.

Chapter 1 investigates the evolving nature of cyber-crime and proposes a framework to determine under what circumstances cyber-crime in securities could pose a systemic risk. **Chapter 2** applies this framework to the results of a survey to the world's exchanges on their current views, experiences and responses to the cyber-crime threat.
Chapter 3 suggests further research and options for engaging with the threat.

[30] World Economic Forum, 2013, 'Insight Report: Global Risks 2013', 8th edition

Cyber-crime covers a broad range of attacks –some more harmful than others and some more criminal than others. A report from KPMG[31] points out that there are two leagues of cyber-crime – a junior league where crimes are 'a nuisance' but with limited impact; and a major league, which threaten critical systems, processes and infrastructure and with potentially more long-lasting and systemic impacts. So far, cyber-attacks against the financial system have displayed little capability for global shock,[32] but historic instances may not, in this case, be a sound basis for predicting future safety. Motives, capabilities and vulnerabilities can quickly change as cyber-criminals of all stripes, rapidly innovate.[33] Thus, it is worth defining whether and under what circumstances cyber-crime in securities markets could pose a systemic risk.[34] To guide such an analysis, the following 'systemic risk impact factors' are proposed:[35]

- **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**

Factors for assessing the cyber-crime risk in securities markets

Using these criteria, a forward-looking investigation into the nature and potential impact of cyber-crime in securities markets can be undertaken, with insights into the magnitude of the risk it could pose to the financial system. Since there is limited data on cyber-crime across securities market actors to comprehensively assess the likelihood of any consequences manifesting, this section proposes a number of 'indicators' that could be used to monitor trends and vulnerabilities, going forward. The next chapter will also provide a preliminary assessment of the cyber-crime risk for exchanges, based on these criteria.

♦ Factor 1: Size of the threat

Analysis of how widespread and common cyber-crime is (for example frequency of attacks and number of targets) can assist in identifying growth trends and in pinpointing particularly vulnerable points - those sections or types of actors in securities markets, which are most targeted. In monitoring the size of the cyber-threat, the following indicators could be used:

[31] KPMG, 'Shifting View', 2012
[32] Peter Sommer, Ian Brown, 'Reducing Systemic Cybersecurity Risk', OECD/IFP Project on 'Future Global shocks', *OECD,* 2011
[33] As the former Director General of MI5, Jonathan Evans stated: "…So far, established terrorist groups have not posed a significant threat in this medium, but they are aware of the potential to use cyber vulnerabilities to attack critical infrastructures and I would expect them to gain more capability to do so in future.", Speech at the *The Mansion House, 2012*
[34] The Financial Stability Board defines systemic risk in the financial system as "*the risk of disruption to the flow of financial services that is (i) caused by an impairment of all or parts of the financial system; and (ii) has the potential to have serious negative consequences for the real economy*".
[35] Based on market intelligence and literature review; and IOSCO Research Department, 'identifying systemic risk in securities markets', Staff Working Paper, 2012. [www.iosco.org/research]

- Number of securities market targets, categorized by type of actor (e.g. hedge fund, exchange etc.)
- Average frequency of attacks on each security market actor per year;[36]
- The percentage of critical services and sensitive information of securities market actors online;
- The average costs (direct and indirect) incurred by securities market actors due to cyber-crime.

In the financial sector, it is clear that cyber-crime is already noteworthy. IOSCO Research Department Market Intelligence revealed broad concern from market participants over the threat. Furthermore, a 2011 PWC survey[37] ranked cyber-crime as the 2nd most commonly reported type of economic crime for financial sector organisations, accounting for 38% of economic crime incidents in 2011; in a survey by Marsh and Chubb, [38] 74% of financial services respondents categorized cyber-crime as a high or very high risk; and a 2013 Verizon report on data breaches noted that more than one third of all breaches reported in the year of 2012 affected financial organizations. [39] The larger economic, political and societal context may also be exacerbating the size of cyber-crime. For example, 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 organisation).[40]

For securities markets specifically, the threat is also palpable. Markets differ perceptibly from the markets of the recent past. Only 20 years ago trading floors were dominated by paper trades, and 'securities' were carried around in briefcases. Now markets are becoming increasingly digitized, with sensitive data and critical processes being moved to computer-based platforms connected to a vast cyberspace. A number of securities market actors, including exchanges and banks, have already become victims of cyber-crime. For example:

- A recent attack on UK bank websites injected fake input fields and security warnings into an otherwise secure website in order to extract passwords and other sensitive information from users.
- In 2012, hackers targeted the websites of the world's largest banks, overloading the servers with requests so that the bank's customers were unable to access the bank's online services. [41]
- An attack on an exchange used malware to gain access to a sensitive application, which stored potentially market moving information on Fortune 500 companies.
- The websites of a number of stock exchanges around the world have faced distributed denial of service cyber-attacks, which flood the system with requests overloading the server and in some cases forcing trading to stall for a brief period. However trading

[36] It is important to distinguish what constitutes a single attack e.g. each individual hit on an institution, or a grouping of hits if they are from the same source.
[37] PWC, "Fighting Economic Crime in the Financial Services Sector", Survey, 2012
[38] Marsh and Chubb, Cyber Risk perceptions: An industry snapshot, Cyber Survey, June 2012
[39] Verizon, 2013 Data Breach Investigations Report
[40] Global Industry Analysts, Inc, 2011; Resilience in the Cyber Era: Building an Infrastructure that secures and protects, Economist Intelligence Unit and Booz Allen Hamilton, 2011
[41] For example See, CNN, David Goldman, 'Major banks hit with biggest cyberattacks in history' [http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html]

platforms have not been directly breached, since exchanges usually have segregated platforms for trading and web-services to prevent systemic contagion. These attacks appear to have a range of motivations – from political and hacktivist interests to corporate interests.

- Attack against the National Market System (NMS) in the United States.[42] After a cyber-attack made corporate filing information unavailable, securities became illiquid and trading had to be halted. This *"negatively impacted both individual and institutional investors in that market*."[43]

While there is limited data available on the costs of cyber-crime for securities markets, a number of studies have calculated costs of cyber-crime to society as a whole – suggesting figures between $388 billion[44] to $1 trillion[45] *so far*. However, costs may vary considerably by segment and sector, [46] [47] making it difficult to extrapolate general results across all securities market actors.

♦ Factor 2: Complexity

When assessing the risk posed by cyber-crime, it is important to distinguish between simple and complex attacks. The complexity of attacks can provide information about the resources of cyber-criminals and depth of attacks. Simple attacks are more likely to be detected quickly with impacts mitigated. More complex attacks may take longer to detect, with longer-term impacts – and may imply quite sophisticated capabilities on the side of the cyber-criminal. Thus, in securities markets, potential indicators should also track:

- The complexity of techniques used, especially those used most commonly;
- The percentage of attacks utilizing social engineering;
- Average detection times for complex attacks.

In the financial system cyber-attacks are reported as more sophisticated than ever, with attacks coming from not only fraudsters but political activists aiming to disable financial institutions.[48] Cyber-attacks can involve various stages of implementation (monitoring, real-world physical interaction, distraction, information stealing, creation of backdoors[49] etc.) and be executed persistently over a number of years (sometimes to distract from the 'real' attack, sometimes to simply probe for weaknesses). The attacks often combine a variety of traditional

[42] which facilitates structured electronic transmission of securities transactions in real-time.
[43] Mark G. Clancy (DTCC), Speech, House Committee on Financial Services, Subcommittee on Capital Markets and Government Sponsored Enterprises, Hearing on "Cyber Threats to Capital Markets and Corporate Accounts", June 1, 2012
[44] Norton, Cybercrime Report, 2011
[45] The Global Industry Analysts; McAfee, 'Unsecured Economies: Protecting vital information' 2011
[46] Ponemon Institute, 'Second Annual Cost of Cyber-Crime Study: Benchmark Study of U.S. Companies', August 2011 [http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf]
[47] At the same time, there are number of studies questioning the accuracy of survey figures on cyber-crime instances and costs, suggesting both an inflation and deflation of true costs, self-selection bias, vested interest of surveyors to exaggerate the risk or of respondents to underplay risks, undetected attacks and limited accountability for false answers. See Ross Anderson, Chris Barton, Rainer Bohne, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore, Stefan Savage, "Measuring the Cost of Cybercrime", 2012; C. Herley and D. Florfiencio, 'A Profitless Endeavor: Phishing as Tragedy of the Commons', 2008, Lake Tahoe, CA; P. Andreas and K. Greenhill, 'Sex, Drugs, and Body Counts: The Politics of Numbers in Global Crime and Conflict', Cornell University Press, 2010; S.D. Moitra, 'Cyber Security Violations against Businesses: A Re-assessment of Survey Data'; J. Ryan and T. I. Jefierson, 'The Use, Misuse, and Abuse of Statistics in Information Security Research,' Proc. 23rd ASEM National Conference, 2003.
[48] Thomson Reuters Accelus, "Special Report: Cybercrime – how can firms tackle this fast-emerging invisible menace?"
[49] A back door involves creating a pathway into a computer system or network that can be exploited later down the track.

cyber-crime 'techniques' so that if even one form is blocked, another form could get through (See Annex X for a list of techniques).

In addition, social engineering makes it even more difficult for a target to identify an attempted breach before it is too late. Although most users may recognize that viruses can infect their computer if they were to click on a link from an unrecognized email sender, riddled with spelling and grammatical errors, today, cyber-attacks can easily imitate trusted email addresses, text messages, media or websites. The information to make cyber-attacks appear trustworthy can be extracted from social media and other online personal or professional data.[50] In fact, last year Verizon reported that almost one third of cyber-attacks in 2012 involved social engineering.[51]

Especially troubling, is the rise of the 'Advanced Persistent Threats' (APTs),[52] which infiltrate a specific computer or networks through targeted and persistent attacks, orchestrated over many years. The perpetrators behind these attacks tend to be driven by political or ideological motives, rather than financial gain. These attacks slowly chip away at any defences and are constantly scanning for weaknesses.[53] Cyber-criminals entrap users through utilizing sophisticated social engineering and the focus on 'information' rather than 'systems' means that they can be orchestrated without obviously affecting the functioning of a computer or network – even as they steal, manipulate or damage information contained on it.[54] [55] The advanced and stealthy nature of these attacks means that they can go undetected for years.

♦ Factor 3: Incentive structure

The probable motive of attacks (e.g. to disrupt, financial gain etc.) can shed light on expected impact. Attacks perpetrated for short-term financial gain are less likely to disrupt the functioning of the financial system than attacks crafted specifically with the intent to disrupt or destroy. It is difficult to monitor the types of actors and identify the motives involved, unless the cyber-criminals publically reveal themselves (which they sometimes do in the case of cyber-terrorism). As such indicators developed could attempt to categorise the types of impacts e.g. disruptive, financially motivated etc. and map the incentive structure for cyber-criminals e.g. development of a black market.

Since the beginning of wide-spread internet usage for disseminating financial advice and information, securities markets and participants have been forced to weather myriad attempts of online financial theft, fraud and scams.[56] As such, cyber-crime in the financial system is often associated with theft and financial gain. At the same time, the traditional picture of a

[50] Sopohos, 'Security Threat Report 2012: Seeing the threat through the hype', 2012
[51] Verizon, 2013 Data Breach Investigations Report
[52] Advanced Persistent Threats (APTs) are usually directed at business and political targets for political ends. APTs involve stealth to infiltrate a system over a long period of time, without the system displaying any unusual symptoms.
[53] Centre for Financial Markets and Policy, Georgetown McDonough and Booz Allen Hamilton, Roundtable discussion, recommendations for addressing cyber threats, February 21, 2012
[54] Social engineering in a cyber security context refers to the manipulation of human beings in order to gain access to networks, systems and digitized information. Techniques usually exploit natural character traits such as helpfulness, trust, greed, hierarchy, conformity and panic. Importantly, the success of social engineering commonly hinges on a vacuum of information around technological threats and a lack of understanding of the value of information.
[55] McAfee Threats Report: Fourth Quarter 2012, McAfee, 2012
[56] As underlined in Peter C. Hildreth, Testimony before the Permanent Subcommittee on Investigations of the Governmental Affairs Committee, "Securities Fraud on the internet & online trading issues", United State Senate, 22 March 1999.

'hacker' usually involves an individual or small under-resourced group utilizing rudimentary hacking skills.

However today, the playing field is much broader and can include large, powerful and well-resourced groups with destructive political, economic or ideological aims. Potential actors could include:[57]

- criminal groups seeking large-scale financial hauls;
- terrorist groups seeking to hold a government ransom or destroy it;
- ideological or political extremists such as anti-capitalists who may wish to destroy the financial system;
- a nation state aiming to undermine a rival state's economy or to strike out as an act of (cyber) warfare;
- In some cases, cyber-attacks may be operated from somebody on 'the inside' e.g. a disgruntled employee, making it virtually impossible to screen and defend from attacks without the use of an 'air-gap'[58] (which is not feasible for some financial services) and strong vetting procedures for all staff at all levels.

Furthermore, the emergence of a cyber-crime 'black market' is widening the incentive structure of hackers. For example, previously hackers may infiltrate a company's internet presence in order to receive 'kudos' from their fellow hacking community and perhaps even a job from the victim company.[59] However, now hackers can sell information they mine to other actors, or even sell their skills on a cyber-crime 'black market', to do the bidding of others – such as nation states or terrorist groups with more political and potentially destabilising aims. This new market for cyber-crime is, by some accounts, becoming a lucrative and well-supported business: manuals, troubleshooting and 24 hour customer service is offered with malware purchase.[60]

♦ Factor 4 & 5: Effect on market integrity and efficiency; Infiltration of non-substitutable and/or interconnected services

Cyber-attacks in our complex, leveraged and interconnected financial system could be disruptive – potentially aiming to choke essential financial services; steal/damage/manipulate information, money supply and markets; [61] damage the capability of the private sector to

[57] See John Bassett, David Smart, "Cyber-attacks on the stock exchange: Threat, motivation and response", www.rusi.org.

[58] An air-gap is where particularly sensitive IT infrastructure severs all connectivity with the general internet or any online service or any devices that have connectivity with the internet e.g. blackberries. Instead it operates within its own closed network.

[59] KPMG, 'Shifting View', 2012 http://www.kpmg.com/TT/en/IssuesAndInsights/ArticlesPublications/Documents/Nuanced-Perspective-on-Cybercrime-Art.pdf

[60] RSA, '2012 Cybercrime Trends Report, 2012 [http://www.rsa.com/products/consumer/whitepapers/11634_CYBRC12_WP_0112.pdf]

[61] For example, the House Committee on Financial Services, Subcommittee on Capital Markets and Government Sponsored Enterprises, Hearing on "Cyber Threats to Capital Markets and Corporate Accounts", Mark G. Clancy (DTCC) , Speech, June 1, 2012 describes how market manipulation can have wide-spread impact on investor confidence and lead to complicated legal binds. Theft of information or funds directly from customers (i.e. via malicious software on a personal computer) on a large scale (thousands, millions of individual account holders) can lead to 'pump and dump' scams, which allow cyber criminals to "*run up the price of a thinly-traded security they own by creating buy and sell orders in the accounts they have taken over*" By bidding against themselves, and luring other investors, they can move the market in the stock they invest in."; also in Alexander F H Loke, "The Internet and Antifraud Regulation of Securities Markets", *Singapore Journal of International & Comparative Law, Vol 5, 2001* reports how some can push false or misleading information via websites and mailing lists in order to manipulate stock prices, due to the speed of penetration of information in the market.; and; Furthermore, one of the few papers on cyber-crime and securities markets by Christina Parajon Skinner ("Cybercrime in Securities Market: Is U.C.C Article 8 Prepared", November 2011) points out how the unauthorized selling off a substantial number of securities to legitimate buyers can lead to problems in properly allocating

ensure orderly functioning of the economy and delivery of services; [62] and severely damage investor confidence.[63] One recent example involves an ATM heist, which managed to accumulate US$45 million through tens of thousands of withdrawals from over 26 countries. The attack not only involved hacking accounts but removed limits on prepaid debt cards – essentially creating money. Such an attack on a grander scale could have an effect on money supply and the real economy.[64]

Attacks can thus reduce market integrity and efficiency. This is especially true of attacks against systemically important institutions, critical financial infrastructures and/or providers of essential (non-substitutable) services, since a significant portion of funds and investors are 'locked into' these institutions and their interconnected nature may facilitate contagion. A pattern of attack may also take form (rather than random attacks), where more than one of these institutions is attacked simultaneously. Potential indicators to consider here include:

- Number of attacks on systemically important institutions and critical/core financial infrastructures;
- Observation of distributed patterns of attack (i.e. hitting multiple securities market actors providing a particular service, at the same time);
- Number attacks that affect data integrity;
- Number of attacks that affect the functionality, availability and/or accessibility of markets

The interconnectedness and complexity of securities markets makes it difficult to pinpoint all the relationships between infrastructures and thus always project how an attack or failure of one component (due to cyber or physical incidents) will affect others.[65] Possible negative impacts on market integrity and efficiency could be achieved through, for example:

- Numerous attacks against the integrity and functioning of a particular technology system of an essential and non-substitutable service, to the point that it "*is rendered too unreliable or error prone to be used for mission critical functions*".[66]
- Tampering with a payment system so its functioning is impaired. This may increase transaction costs, which will in turn be reflected in prices and which may impact the *"efficient matching of buyers and sellers*".[67]
- Breaking trust in the confidentiality of data through breaching numerous firms (big or small) and leaking information.[68]

---

ownership rights. Uncertainty over ownership could slow or halt trading and result in investor hesitation. This could have related liquidity and credit issues.

[62] U.S. Government, White House, Homeland Security, Presidential Directive 7: *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003, [see http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#content.]

[63] *"a security breach at one firm can create negative ripple effects that greatly impact systemic risk in financial markets" in* Booz Allen, top ten cyber security trends for financial services in 2012, 2011

[64] Ross Dawson, Interview on SBS 6.30 news, May 11, 2013.

[65] Lior Tabansky, "Critical Infrastructure Protection against Cyber Threats", *Military and Strategic Affairs,* Vol 3, no. 2, Nov 2011

[66] Centre for Financial Markets and Policy, Georgetown McDonough and Booz Allen Hamilton, Roundtable discussion, recommendations for addressing cyber threats, February 21, 2012

[67] Mark G. Clancy (DTCC) , Speech, House Committee on Financial Services, Subcommittee on Capital Markets and Government Sponsored Enterprises, Hearing on "Cyber Threats to Capital Markets and Corporate Accounts", June 1, 2012

[68] Mark G. Clancy (DTCC) , Speech, House Committee on Financial Services, Subcommittee on Capital Markets and Government Sponsored Enterprises, Hearing on "Cyber Threats to Capital Markets and Corporate Accounts", June 1, 2012

Attacks against multiple core financial infrastructures or any providers of non-substitutable services, could have knock-on or cascading effects[69] even if the attack has limited impact on the actual victim institution.[70] Cascading effects refer to downstream impacts of information/system failure/degradation, such as on secondary systems or infrastructures. [71] If multiple targets are hit, seemingly manageable issues (such as: transactions not being completed, employees not being paid, incorrect information being transmitted) could cumulate into a far less containable risk. [72] [73] [74]

Furthermore, cyber-attacks specifically tailored for only a few large or critical entities are more difficult to detect and defend against. When cyber-attacks are launched against a wide array of potential victims, it is easier to notice a pattern and erect barriers in detection systems and anti-virus software. However, since standard anti-virus software technologies can only detect and prevent what they know of, they may prove insufficient in the face of 'zero-day'[75] or more tailored attacks. [76]

♦ Factor 6: Awareness and Transparency

An environment of low awareness and transparency (e.g. through lack of information sharing arrangements) could exacerbate the impact of cyber-attacks. A lack of awareness may mean that actors are more likely to be 'blindsided' by a new attack and find themselves without the appropriate tools and protocols to mitigate damage. Furthermore, where there is a lack of transparency around emerging forms of cyber-crime, there could be a hidden build-up of risk. Potential indicators around transparency to consider include:

- Perceptions of Board level buy-in and understanding of the cyber-risk to their institution. This is especially important since senior management are normally the ones privy to what data/information is most valuable or sensitive;[77]
- Percentage of organizations where senior management are actively aware of attack instances;
- Percentage of actors sharing information with other private sector actors and authorities on attacks (successful and otherwise);
- Percentage of actors sharing information cross-jurisdictionally;
- Percentage of actors that use cross-jurisdictional information sharing centres/partnerships

In the financial sector, experts consulted during market intelligence expressed concern that the Boards of prominent financial firms and organizations are neither engaged with cyber-

[69] Keshav Dev Gupta and Jitendra Joshi, "Methodological and Operational deliberations in Cyber-attack and Cyber exploitation International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Iss 11, November 2012
[70] Mike McConnell, Speech, Meeting of the American Bar Association standing committee on law and national security.
[71] Lior Tabansky, "Critical Infrastructure Protection against Cyber Threats", *Military and Strategic Affairs,* Vol 3, no. 2, Nov 2011
[72] W. Shane Powell, Methodology for Cyber Effects Prediction, 22 January 2010 http://www.blackhat.com/presentations/bh-dc-10/Powell_Shane/BlackHat-DC-2010-Powell-Cyber-Effects-Prediction-wp.pdf
[73] Scott Borg, Economically Complex Cyber-attacks, Security & Privacy, IEEE, 2005
[74] While the same could be said for physical attacks which are already acknowledged, cyber-crime is unique in that it is relatively easier and less resource-intensive to carry out (then a physical attack) and does not require geographical proximity.
[75] A zero day attack is one that exploits an unknown vulnerability.
[76] ENISA, Flash Note, *Cyber-attacks – a new edge for old weapons*, 13 March 2013.
[77] Lior Tabansky, "Critical Infrastructure Protection against Cyber Threats", *Military and Strategic Affairs,* Vol 3, no. 2, Nov 2011; KPMG, 'Shifting View', 2012 http://www.kpmg.com/TT/en/IssuesAndInsights/ArticlesPublications/Documents/Nuanced-Perspective-on-Cybercrime-Art.pdf

security nor aware of the threats posed by cyber-crime. In a recent PWC survey, most financial service respondents reported cyber-crime as an issue to be dealt with by their IT departments. [78] Furthermore, a Marsh and Chubb survey revealed that 75% of financial services executives were unaware as to whether their company had even been the victim of a cyber-attack.[79] Awareness may vary across different groups of financial market actors however. For example, these findings contrast with the high levels of awareness revealed across surveyed exchanges (see pg. 29).

Even armed with awareness of the cyber-threat, it is sometimes difficult to distinguish between legitimate cyber threats, 'nuisances' and even accidents, especially in the immediate aftermath – or worse: cyber-criminals may use these 'nuisance' attacks to effectively distract public view from a more malicious threat. Nevertheless, once news of a potential 'attack' is released into the public sphere, the company or organization will face pressure to allocate resources towards engaging with the attack.

Market actors may face a dilemma in trying to avoid a slow public response to a cyber-attack due to taking the time to conduct forensic analysis of the threat, which can heighten panic in the long run and lead to fines for inaction,[80] and taking immediate but unqualified action which may starve resources from dealing with more legitimate threats.

Knee-jerk responses could also worsen the impacts of an attack where actors flood markets with, sometimes irrelevant, information targeted at calming fears in the wake of an attack but actually cause price inefficiencies due to the elevated and unnecessary information processing needed. [81] [82] Yet, a lack of transparency may fuel panic in the market,[83] amplifying cascading effects to other actors. Investor's may feel the market is 'out-of-control' or that they have been 'tricked' – even if the issue is resolved quickly through strong disaster recovery practices. [84] This could result in retreat from the market and force inefficient investment or misallocation of resources by victim firms as they try to battle ruined reputations. In fact, reputational damage is often cited as the most concerning consequence from cyber-crime for financial actors, more so than direct financial loss.[85]

Insufficient information sharing between public and private actors can also limit abilities to properly engage with, understand, investigate, prosecute and warn other actors about emerging cyber-crime risks. [86] The potential for reputational damage from sharing information

[78] PWC, "Fighting Economic Crime in the Financial Services Sector", Survey, 2012
[79] Marsh and Chubb, Cyber Risk perceptions: An industry snapshot, Cyber Survey, June 2012
[80] For example, a cyber-attack on Sony Playstation in 2011, where hackers stole personal information of 77 million users, resulted in a 250 000 pound fine on the company. The company was accused of breaching the UK Data Protection Act by having insufficient preventative and security measures in place. Furthermore, Sony came under fire for their slow response time in informing customers of the breach.
[81] Christina Parajon Skinner, "Cybercrime in Securities Market: Is U.C.C Article 8 Prepared", November 2011
[82] As investors exert substantial effort in understanding the cyber-threat landscape before purchasing securities, the price of securities may be undervalued.
[83] Booz Allen Hamilton and Georgetown University, "Cyber security Threats in Financial Services", Roundtable Summary, February 2012.
[84] For example, a cyber-attack on Sony PlayStation in 2011, where hackers stole personal information of 77 million users, resulted in a 250 000 pound fine on the company. Sony came under fire for their slow response time in informing customers of the breach.
[85] PWC, "Fighting Economic Crime in the Financial Services Sector", Survey, 2012
[86] RSA, '2012 Cybercrime Trends Report, 2012 [http://www.rsa.com/products/consumer/whitepapers/11634_CYBRC12_WP_0112.pdf]; Resilience in the Cyber Era: Building an Infrastructure that secures and protects, Economist Intelligence Unit and Booz Allen Hamilton, 2011; Centre for Financial Markets

with the public or authorities, fear of penalty, and privacy concerns over intellectual property may be factors in stopping actors from reporting a cyber-breach. Even though a number of jurisdictions have regulations in place to ensure free flow of information between the private and public sector[87] and there are a number of centres and public-private partnerships set up to facilitate information sharing,[88] there is little in the way of formal arrangements for cross-border information sharing nor is there an international code of conduct for cyber investigations.[89]

Yet, cyber-crime does not recognize state borders. In the absence of clear cross-jurisdictional information sharing arrangements, authorities, regulators and information providers may not be able to retrieve the necessary information on attacks and attack trends, especially if critical information of an attack's architecture or signature is held on servers in another jurisdiction with strict privacy laws.

♦ Factor 7: Level of cyber security and cyber-resilience

Robust cyber-security (detection and prevention) and cyber-resilience (ability to continue functions and/or bounce back quickly during and after an attack) are important factors in mitigating impacts from cyber-crime. Non-existent or ineffective cyber-security and cyber-resilience creates a tempting opening for 'would-be' cyber-criminals and may mean that even relatively simplistic cyber-attacks can get in and cause damage. Potential indicators to consider include:

- Presence of cyber-security and cyber-resilience across all securities market actors;
- Perceptions of effectiveness of cyber-security and cyber-resilience measures;
- Detection speeds;
- Repeated staff training;
- Resourcing of cyber-security as percentage of IT budget and percentage of full-time IT staff;
- Evidence of engagement with cyber-physical threats e.g. a merged group to handle cyber and physical security.

Cyber-security measures in securities markets should be proactive (attempting to anticipate new forms of risk and potential vulnerabilities) as well as reactive.[90] Reliance only on 'reactive'

---

and Policy, Georgetown McDonough and Booz Allen Hamilton, Roundtable discussion, recommendations for addressing cyber threats, February 21, 2012

[87] For example the SEC in the U.S.

[88] For example, in the **U.S.:** The U.S. Internet Corporation for Assigned Names and Numbers (ICANN) in 2006; the National Cyber Security Alliance campaign in 2010. The Financial Services-information sharing and analysis centre (FS-ISAC) was launched in 1999 to gather and disseminate information to members in relation to both cyber and physical threats; the Financial Services Sector Coordinating council for Critical Infrastructure Protection and Homeland Security (FSSCC), established in 2002 and with 52 members representing the financial industry – from banks to clearing houses to financial utilities. NCFTA, an alliance between the FBI, U.S. Postal Inspector and Private Industry. The U.S. Department of Homeland Security has set up the Multi-State Information Sharing and Analysis Centre (MS-ISAC) and National Association of State Chief Information Officers (NASCIO). In **Europe**: The London Action Plan represents cooperation between Telecommunication providers, Consumer public Authorities and industry. The European Financial Coalition involves cooperation between law enforcement, IT and industry (financial). In the UK, a 'virtual task force' has been set up to act as a forum on cyber security issues and build trust between authorities and firms and just recently the British secret service has set up a new secret unit involving around 160 private companies, government officials and intelligence personnel.

[89] Jami Shea, Deputy Assistant Secretary General, 'Emerging Security Challenges', NATO [http://www.europesworld.org/NewEnglish/Home_old/Article/tabid/191/ArticleType/ArticleView/ArticleID/21940/language/en-US/Default.aspx]

[90] Richard Colbaugh and Kristin Glass, "Proactive Defence for Evolving Cyber Threats", *Sandia Report*, November 2012

preventative mechanisms such as firewalls, antivirus and intrusion detection systems is no longer sufficient. This is because many of these sorts of mechanisms are 'signature based', which means that a particular form of virus, malware etc. must be widespread, identified and then logged before it can be protected against. There will always be some customers suffered as collateral, before the anti-virus software can notice the new threat and update. Previously unknown threats can thus filter through standard defense mechanisms undetected, especially if the attack is tailored for a single target entity.

In addition, cyber-attacks do not only target technological vulnerabilities, but vulnerabilities arising from the behaviour of staff, suppliers and clients. Even with robust cyber-security measures in place, a single organization may find it difficult to control the cyber-security practices of its suppliers and any outsourced services.[91] Furthermore, cyber-security measures could be easily side-stepped if the crime is perpetrated by an 'insider' (an employee).

Human users are often the most vulnerable and unpredictable part of a firm's technological infrastructure and by taking advantage of the 'human element' of cyber systems rather than exploiting technological or network weakness, the threat becomes almost impossible to eliminate. Training for all staff (not just IT staff) is important and given the innovation of cyber-crime, training is best executed periodically (rather than a one-off) with staff being kept up-to-date on new threats.

Nevertheless, prevention and detection alone is not sufficient, [92] robust cyber-resilience is also important. [93] Cyber-resilience refers to the ability for technological infrastructure and a firm's reputation, critical operations etc. to continue during (or recover quickly) after a successful attack.[94] Cyber-resilience can be facilitated through clear disaster recovery protocols and can be considered as a subset of business continuity.[95] Having clear protocols in place can be essential in maintaining stability of an organization, but can also assist in ensuring the stability of the greater financial system – by mitigating reputational damage (through appropriate public relations); notifying others that could also be affected by a cyber-attack e.g. customers, connected partners and members of the supply chain; and mitigating financial/information loss through use of external back-up systems (although these may be just as vulnerable to cyber-attacks). [96] Cyber insurance, while perhaps not useful in ensuring functioning during and in the immediate aftermath of an attack, can assist in cost recovery over the longer-term.

A number factor to consider is cyber-physical attacks, where cyber and physical attacks are perpetrated in tandem. According to the Verizon 2013 report on data breaches, more than one third of cyber-attacks involved physical attacks.[97] This is not surprising considering the clear overlaps between the physical and cyber world. If a virus is spread through a computer

[91] Barney Jopson, "Cybercrime link to outsourcing", Financial Times, 25 March 2013

[92] KPMG, 'Shifting View', 2012 http://www.kpmg.com/TT/en/IssuesAndInsights/ArticlesPublications/Documents/Nuanced-Perspective-on-Cybercrime-Art.pdf

[93] House Committee on Financial Services, Subcommittee on Capital Markets and Government Sponsored Enterprises, Hearing on "Cyber Threats to Capital Markets and Corporate Accounts", Mark G. Clancy (DTCC) , Speech, June 1, 2012

[94] Nigel Inkster, Director of Transnational Threats and Political Risk at the International Institute for Strategic Studies in Resilience in the Cyber Era: Building an Infrastructure that secures and protects, Economist Intelligence Unit and Booz Allen Hamilton, 2011

[95] Disaster Recovery, a subset of business continuity, involves designing plans of action and processes for ensuring continuation of critical operations in the face of both small and large events, and fast recovery in the wake of a 'disaster'.

[96] KPMG, 'Shifting View', 2012 http://www.kpmg.com/TT/en/IssuesAndInsights/ArticlesPublications/Documents/Nuanced-Perspective-on-Cybercrime-Art.pdf

[97] Verizon, 2013 Data Breach Investigations Report

network by an intruder or an unknowing employee inputting an infected UBS drive or smart phone into a work terminal: is this a physical security issue (intruder, use of hardware etc.), or is it a cyber issue (infected computer network)? It's both. Or: The ID card access unit allowing entry into a building or data centre is disabled through a cyber-attack, allowing unauthorized persons to enter a building and manipulate/steal or damage information, data or technological infrastructure. Is this a physical issue? Or a cyber issue? Again, it's both.[98] Cyber-attacks can also be perpetrated to distract from an impending physical attack, or vice versa. An attack timed to coincide with a non-cyber disaster (natural or otherwise) could severely dampen recovery efforts and facilitate a slide into crisis (a blended threat).[99]

♦ Factor 8: Effectiveness of existing regulation

Currently the international nature of cyber-crime in all sectors makes it difficult to detect, prosecute and/or execute recuperative or responsive action. Jurisdictional conflict and/or ambiguity when it comes to cyber-crime regulation can accentuate possibilities for regulatory arbitrage and create confusion for actors around legal channels to 'fight back' (e.g. counter attacks).[100] [101] Ineffective regulation also means that cyber-criminals are less likely to be deterred. Potential indicators:

- Perceptions on the effectiveness of deterrence and enforcement of regulation;
- Instances of jurisdictional conflicts/ambiguity;
- Possibilities for regulatory arbitrage.

Despite some efforts towards global harmonization in the fight against cyber-crime,[102] there is still jurisdictional fragmentation in terms of definitions, legal frameworks and enforcement actions[103] and there is no global governance mechanism for cyber-crime related cases.[104] There are also legal and political barriers to overcome, especially dealing with a potential criminal from another jurisdiction – due to sovereignty, privacy and human rights.[105]

---

[98] Examples from Gregg La Rouche, 'Information and Physical Security: Can they live together?', Infosectoday, http://www.infosectoday.com/Articles/convergence.htm:

[99] Peter Sommer, Ian Brown, 'Reducing Systemic Cybersecurity Risk', *OECD,* 2011, OECD/IFP Project on 'Future Global shocks',

[100] Ross Anderson, Chris Barton, Rainer Bohne, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore, Stefan Savage, "Measuring the Cost of Cybercrime", 2012

[101] A counter attack involves 'hacking' back against the original cyber-criminals targeting your data or systems; see Jay P. Kesan and Carol M. Hayes, "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace", *Harvard Journal of Law & Technology, Vol 25, no. 2 2012.*

[102] For example: 2011, U.S.-China bilateral cooperation agreement; G8, 1997 Ministers' Communique with action plan and principles to combat cybercrime and ensure data protection, and mandate for law enforcement training; United nations General Assembly Resolutions (2000 and 2002) on misuse of information technology; International Telecommunication Union (ITU-UN) Geneva Declaration of Principles, Geneva Plan of Action and subsequent Tunisia Commitment in 2005 highlighting measures in the fight against cyber-crime; Council of Europe 2001 Convention of Cyber-crime, considered a milestone in international cyber regulation in harmonizing definitions, basis for international cooperation and proposing legal frameworks; Asia-Pacific Economic Cooperation (APEC) Cyber security Strategy of 2002 proposing legal frameworks, information sharing arrangements, technical guidelines and awareness raising and training; OECD 2002 'Guidelines for the Security of Information Systems and Networks; The Economic Community of West African States (ECOWAS) 2009 Directive on fighting cybercrime and which outlines a legal framework; The Association of Southeast Asian nations (ASEAN) saw the signing of the ASEAN-China Strategic Partnership for Peace and Prosperity, including cybercrime measures; Interpol and Europol are in the process of creating a collaborative action plan to combat transnational crime; the UNODC has published guidance in 2012 on investigation and prosecution of internet-related terrorist cases.

[103] The History of Global Harmonization on cybercrime Legislation- The Road to Geneva, Stein Schjolberg, December, 2008

[104] Peter Sommer, Ian Brown, 'Reducing Systemic Cybersecurity Risk, 'OECD, 2011, OECD/IFP Project on 'Future Global shocks', 'Reducing Systemic Cybersecurity Risk'

[105] See Rotenberg, 2010 for an analysis of legal issues; In April 2010 a number of emerging economies including Brazil, Russia, China rejected the European Cybercrime Convention on the grounds that it would violate sovereignty by giving foreign police cross-jurisdictional powers.

An in-depth report into cyber-crime by the UNODC[106] elaborates on some of these issues, essentially pointing out that current national legal frameworks may be unfit to engage with the transnational nature of cyber-crime: *Is the crime considered committed where the victim institution resides, where the servers used to perpetrate the crime are held or where the cyber-criminals originate?* For some cyber-crime cases, numerous jurisdictions may claim authority over handling a cyber-crime act. This may be particularly problematic if cyber-crime offences are treated differently in different jurisdictions. For example, the UNODC reports notes that the production, distribution and possession of cyber-attack tools e.g. malware, is criminalized in some countries but not others. [107] Cyber-criminals may thus take advantage of lax or non-existent cyber-crime laws in certain jurisdictions, even if their attacks are focused towards jurisdictions with stricter rules.[108]

Complicating the situation further, is the issue of attribution. The nature of cyberspace makes it easy to both wipe any identifiers and create fake ones, raising challenges for the correct identification of criminals.[109] Cyber-criminals can also take-over the computers of innocents (without them knowing), in order to carry out their crimes.[110] A false accusation could have political consequences and damage foreign relations, especially if nation state actors are involved. This all makes cyber-crime investigations "complex, lengthy and expensive",[111] and authorities and police may struggle to allocate budget away from localized, physical threats towards these more global, intangible ones.

Systemic risk scenarios

While there is uncertainty around the size of the cyber-crime threat in securities markets, there are clear signs that it is a growing threat to the financial sector, with potential for large costs. Cyber-crime also appears to be increasing in terms of sophistication and complexity, widening the potential for infiltration and large-scale damage. On top of these developments, the incentive structure underpinning cyber-criminals is seeing a disturbing change with new actors entering the fray – ones with more destabilizing motives rather than monetary ones.

Cyber-crime differs from traditional financial risks e.g. liquidity, credit risk. Instead of triggering a bank run, it could result in widespread mistrust and retreat from markets. Disruptive attacks against non-substitutable, systemically important and otherwise interconnected services could have knock-on effects in securities markets and impact market integrity and efficiency.

Yet, awareness of the cyber-crime threat may not be sufficiently widespread amongst the senior executives defence in the financial sector to mount an effective defence and transparency of the risk landscape is constrained by state or regional borders. Regulation and sanctions may also lack efficacy in deterring or prosecuting criminals due to difficulties and tracing, attributing and pursuing criminals across borders.

However, since cyber-crime has had no impact on the stability of the financial system so far, there are challenges in defining how and whether cyber-crime in securities markets is a

[106] UNODC, "Comprehensive Study on Cybercrime", February 2013

[107] UNODC, "Comprehensive Study on Cybercrime", February 2013

[108] Phil Williams, Note, 'Organized Crime and Cyber-Crime: Implications for Business', CERT Coordination Centre

[109] ENISA, Flash Note, *Cyber-attacks – a new edge for old weapons*, 13 March 2013.

[110] Peter Sommer, Ian Brown, 'Reducing Systemic Cybersecurity Risk', OECD, 2011, OECD/IFP Project on 'Future Global shocks' 'Reducing Systemic Cybersecurity Risk'

[111] Peter Sommer, Ian Brown, 'Reducing Systemic Cybersecurity Risk', OECD, 2011, OECD/IFP Project on 'Future Global shocks'

systemic risk.[112] Even with the framework introduced in this paper, there are no recognized thresholds and benchmarks for determining the line between systemic and non-systemic cyber-crime. Despite this uncertainty, data and analysis around the factors proposed here can provide a preliminary understanding of the cyber-crime risk in securities markets and form the foundation of a number of potential 'systemic risk scenarios' - scenarios where cyber-crime could pose a systemic risk.[113]

One obvious potential systemic risk scenario would involve complex cyber-attacks executed with high frequency, against numerous targets (including infiltration of non-substitutable and/or interconnected services), with the motive to disrupt/destabilize and impact the functionality, availability and accessibility of markets and/or data integrity. Insufficient preventative, detection and disaster recovery measures would ensure the attacks infiltrate a significant number of targets and a low level of awareness of the risk and limited transparency of the risk landscape would hinder communications between target firms and the larger market, and dampen attempts to mount a collaborative defence. Ineffective regulation (including opportunities for regulatory arbitrage) could mean the perpetrators remain safe from prosecution and free to continue their attack.

However, the weighting and relationship between the factors outlined in this chapter is dynamic and should be assessed on a case-by-case basis. Sole focus on the size of the threat (i.e. frequency of attacks and number of victims) and type of targets (i.e. systemically important institutions, core infrastructures), over other factors such as the complexity of attacks and other potential impacts on market integrity and efficiency could be misleading.

For example, numerous, complex attacks against smaller, non-systemically important firms could have grave implications for data integrity and investor confidence, impacting market integrity and efficiency. In addition, smaller firms, which may not have the resources for robust cyber-defence,[114] could be used by cyber-criminals as a way to gain access to information or manipulate systems of larger, systemically important firms (e.g. that they service or supply through outsourcing). Such a pattern of attack may be difficult to detect and mitigate without high levels of awareness and transparency of the threat landscape across securities market actors, including the smaller ones.

Another example could include an incredibly sophisticated and disruptive attack against only a few targets. By limiting the victims, the attack may be able to evade detection from standard cyber-security tools long enough to cause damage. If the aim of the attack is to cripple access, availability and functionality of markets, attacks may target providers of essential and non-substitutable services or systemically important (and interconnected) institutions. Cyber-criminals could feel confidence in constructing a particularly destructive attack if there is a negligible change of being caught and facing ramifications.

[112] The Financial Stability Board defines systemic risk in the financial system as "*the risk of disruption to the flow of financial services that is (i) caused by an impairment of all or parts of the financial system; and (ii) has the potential to have serious negative consequences for the real economy*".

[113] For the purposes of this report, a 'systemic risk scenario' refers to the conditions under which a cyber-attack(s) could be considered likely to have systemic implications.

[114] As recognized in Mark G. Clancy (DTCC) , Speech, House Committee on Financial Services, Subcommittee on Capital Markets and Government Sponsored Enterprises, Hearing on "Cyber Threats to Capital Markets and Corporate Accounts", June 1, 2012

This chapter sheds some light on the current state of cyber-crime in securities markes and potential for future impacts, by applying some of the systemic impact factors and indicators outlined in Chapter 1 to the experiences and perceptions of the world's exchanges.

The WFE/IOSCO survey to the world's exchanges

In order to gather unique insights and data around the cyber-crime risk from a securities market perspective, the IOSCO Research Department, jointly with the World Federation of Exchanges Office, conducted a cyber-crime survey (See Box 2 for details on the survey) to some of our core financial market infrastructures - the world's exchanges. [115]

The focus on exchanges is not due to any particular or perceived vulnerability to cyber-crime, in comparison to other groups. Rather, this survey acts as the first part of a series of surveys aimed at exploring experiences and perspectives on cyber-crime across different types of securities market actors. Exchanges are also a key regulatory focus for IOSCO members, serving an important function in providing a platform for trading and issuing securities. In some cases, exchanges may operate other critical financial market infrastructures such as payment clearing and settlement processes (e.g. Central Counterparties)[116] and these other processes play a vital role in maintaining financial stability but can also contribute to vulnerabilities by concentrating risk in the financial system and sourcing/transmitting contagion and financial shocks. [117] Exchanges also have the distinction of being 'visible' and prominent in the public psyche when it comes to conceptualising the financial system.

The results of the survey are reported along the following themes

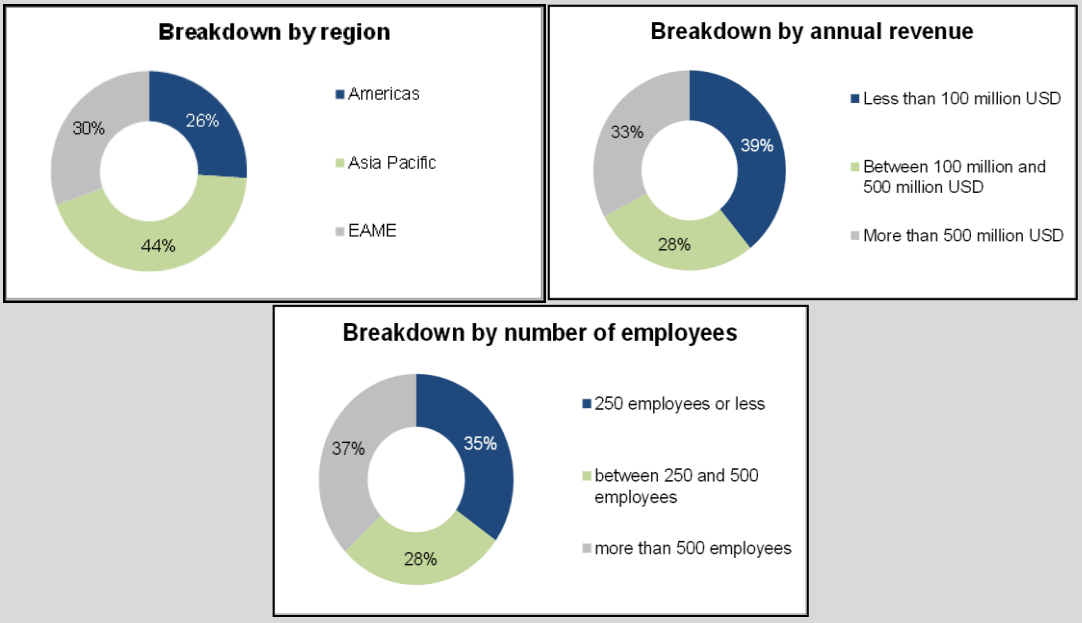
1. Size, complexity and incentive structure
2. Effect on market integrity and efficiency and infiltration of core infrastructures
3. Level of Awareness and Transperency
4. Level of cyber-security and cyber-resilience
5. Effectiveness of existing regulation

[115] Survey undertaken end 2012/early 2013
[116] CPSS/IOSCO, Principles for financial market infrastructures, April 2012 [http://www.bis.org/publ/cpss101a.pdf]
[117] CPSS/IOSCO, Principles for financial market infrastructures, April 2012 [http://www.bis.org/publ/cpss101a.pdf]

Box 2: The WFE/IOSCO Survey

- The 2012-13 Cyber-Crime Survey to the World's Exchanges was conducted jointly by the IOSCO Research Department and World Federation of 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 were moulded around specific concerns and insights gleaned from 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 from the world' exchanges and CCPs, constituting a 75% response rate. Distribution of response by organization size (annual revenue), number of employees and region are provided in Figure 1.
- 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.

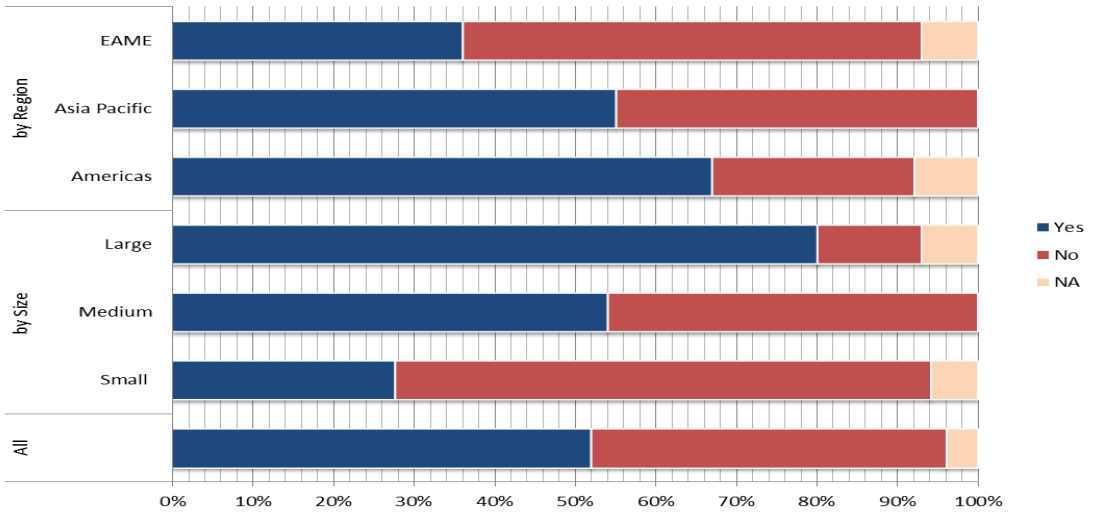
Diagram 1: Distribution of Respondents



♦ *Theme 1: Size, complexity and incentive structure*

A significant number of exchanges have been attacked in the last year. Over half of exchanges surveyed (53%) reported suffering an attack in 2012 (See Figure 1). Exchanges from the Americas were more likely to report having suffered an attack (67%).

Figure 1: Has your organization suffered a cyber-attack in the last year?



Direct financial costs suffered so far are negligible. [118] To the question 'What would you estimate as the monetary impact, both direct and indirect, of cyber-attacks to your organization in the last 12 months? All respondents indicated 'less than 1 000 000' USD.

More information is needed on the complexity of attacks. Attacks against exchanges most frequently involve Denial of Service attacks and use of malicious software.[119] While malicious software can be sophisticated in nature, Denial of Service attacks have traditionally not been considered complex attacks, although they are seeing increasing sophistication in terms of their disruptive capabilities – especially in use against the financial sector.[120] Further information is needed to properly assess the sophistication of these attacks.

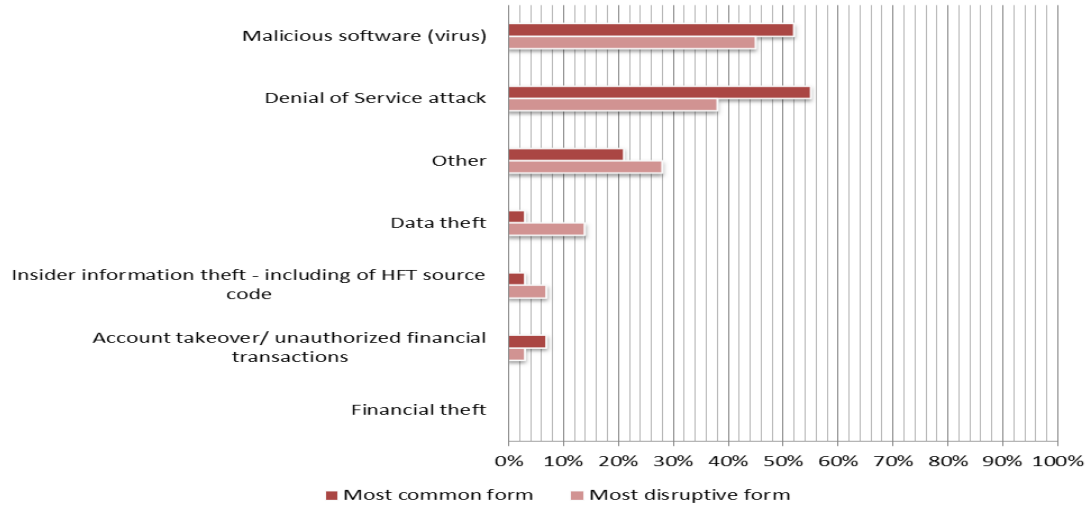
Exchanges tend to be victims of 'disruptive' forms of cyber-attack, rather than those executed for financial gain. While it is difficult to pinpoint the motives of cyber-criminals, in the WFE/IOSCO Survey, there is high correlation between the categories selected as the most disruptive form of cyber-attack, and the categories selected as the most common form of cyber-attack experienced: *Denial of Service attacks* and *Malicious software (viruses)* (see Figure 2). *Financial theft* did not feature in responses to these categories. This suggests that disruption rather than financial gain, featured as a motive for cyber-criminals.

[118] To the question 'What would you estimate as the monetary impact (both direct and indirect) of cyber-attacks to your organization in the last 12 months? All respondents indicated 'less than 1 000 000 USD'

[119] These forms of attack also featured in responses as potentially hazardous forms of cyber-attack for exchanges.

[120] IBM X-Force 2012 Annual Trend and Risk Report

Figure 2: Most common and most disruptive form of cyber-attack?



'Other' forms of common attacks reported related to: SQL Injection, Laptop Theft, Website Defacement attempts, Port scanning and spam emails, Phishing email attack, social engineering, Website scanning.

'Other' forms of disruptive threats included: Website defacement attempts, Port scanning and spam emails, Self-replicating email virus, Advanced Persistent threats, infrastructure damaging threats.

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

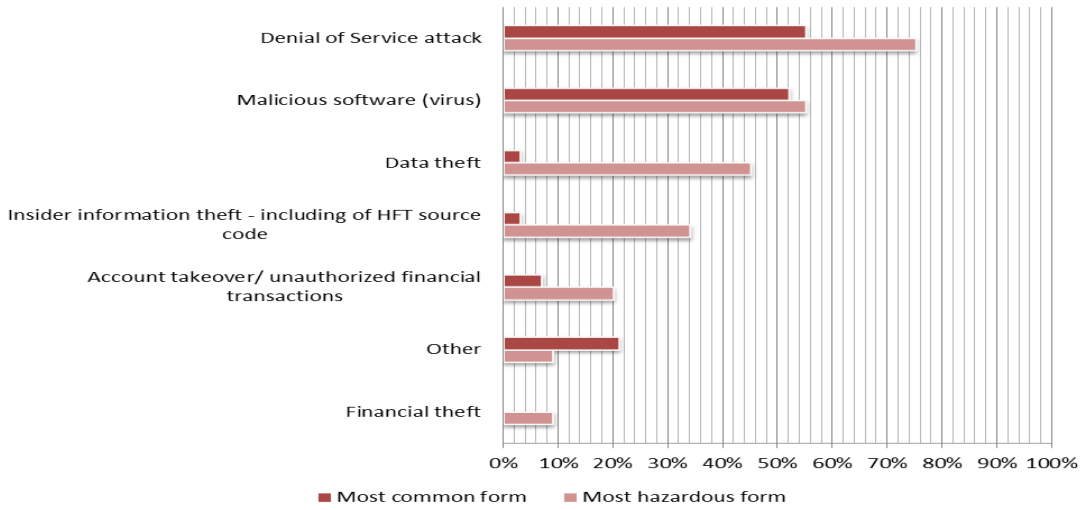
Attacked exchanges are part of our core financial infrastructure and are also interconnected providers of essential (and non-substitutable) services. Large exchanges were most likely to report having suffered an attack (80%), although smaller exchanges were not immune (see Figure 1 above). The combination of low redundancy (few substitutes to perform similar functions); high and cross-sectorial interdependency; and near monopoly (a small number of players providing the same critical service) of exchanges could heighten the systemic consequences of failure from a cyber-attack.[121] [122]

However, so far cyber-crime on exchanges has had no impact on market integrity and efficiency. The type of attacks most frequently selected as 'potentially most hazardous' also correlated with the most common form of attacks experienced – denial of service attacks and malicious software. Data theft and insider information theft (including of HFT source code) were also frequently selected as hazardous forms of cyber-crime but were not common across a significant number of exchanges (see Figure 4). Respondents noted that attacks focused on damaging public facing, non-trading related online services and websites but that none had come close to knocking out critical systems or trading platforms. Many respondents also noted that most of the costs associated came from dealing with reputational fall-out and trust in the wake of an attack.

[121] Peter Sommer, Ian Brown, 'Reducing Systemic Cybersecurity Risk', OECD, 2011, OECD/IFP Project on 'Future Global shocks',; Scott Borg, Economically Complex Cyberattacks, Security & Privacy, IEEE, 2005

[122] Presentation by Peter Daly, 'Banking and Finance', Commissioner, President's Commission on Critical Infrastructure Protection.

Figure 4: Most common and most potentially hazardous form of cyber-attack to exchanges?



'Other' forms of common attacks reported related to: SQL Injection, Laptop Theft, Website Defacement attempts, Port scanning and spam emails, Phishing email attack, social engineering, Website scanning.

Other' hazardous threats to organisation mentioned were: website defacement, client access network testing security failures, laptop theft, targeted email attacks, data manipulation and threats to data integrity.

A number of respondents could envision a large-scale, coordinated and successful cyber-attack on financial markets having a substantial impact on market integrity and efficiency. Respondents to the WFE/IOSCO survey were asked to define, in their own words, what a large-scale, coordinated and successful attack on securities markets could look like (see Figure 5 for excerpts). While some answers flagged smaller impact scenarios such as 'temporary disruption to financial web-based services', the majority of respondents proposed scenarios with more far-reaching consequences, such as:

- Halting trading activity;
- Targeting telecommunication networks in order to compromise availability and accessibility to markets;
- Data manipulation/compromise of data integrity;
- Leaking of insider information on an ongoing basis;
- Affecting ability of a clearing house to act as a central counter party within the settlement window;
- Ongoing disruption of the market and compromise of integrity in order to lower confidence and reputation of the financial actors;
- Infiltration of multiple exchanges using a range of different types of cyber-attack techniques in tandem.

Figure 5: Define what a large-scale, coordinated, successful cyber-attack on financial markets could look like.

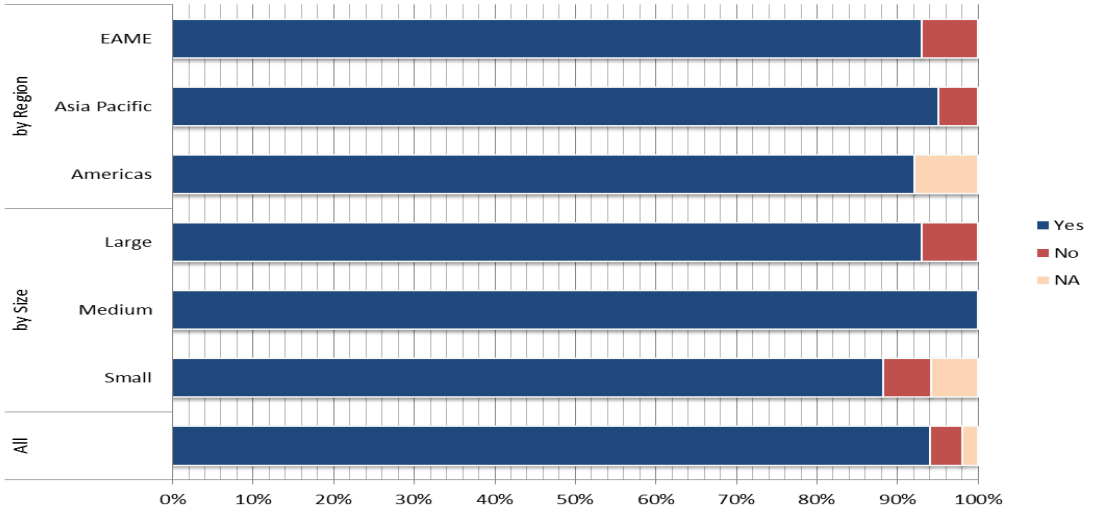
Response Excerpts

- *"…a large scale Denial of Service attack against a range of parties while already installed malware is used to steal data or cause damage to systems or their credibility. Alternatively malware could be used to infiltrate corporate networks to steal data on an on-going basis for financial gain."*
- *"The worst type of attack would be an advanced persistent threat where compromise is not detected and information is compromised or leaked over a period of time without detection giving advantage to certain market participants, circumventing regulatory control measures, corporate espionage as well as data manipulation over a period of time going undetected."*
- *"A systemic risk scenario might involve infiltration of several exchanges, probably most easily by email phishing campaigns involving stealth malware, access built up and maintained over a length of time, potentially involving contractors or malicious inside employee assistance, and over time enough reconnaissance done to identify key internal systems attackable from the infiltration point, and a coordinated attack from that internal toe-hold against multiple institutions. Clever attackers would probably mask such real threats with the noise of the traditional network based DDOS's we've seen in prior years."*
- *"… Given the more exposed nature of market participants, a successful attack would involve the compromise of participant systems. From there, order flow may be affected and malicious injects created and deployed."*
- *"A well organized, well designed campaign designed to strategically impact national market systems - especially in terms of liquidity. Such an effort would require detailed knowledge of national market systems and operations within specific FIs (insider threat/collusion) combined with advanced/multifaceted cyber-attack plan targeting the availability and/or integrity of key resources."*

♦ *Theme 3: Level of transparency and awareness*

There is a high level of awareness across the world's exchanges. Nearly all exchanges surveyed (93%) report that cyber-crime is generally understood and discussed by the senior management (see Figure 6). As well as senior executive buy-in, there are clear upward reporting lines present in the majority of exchanges. The general information security reporting structure appears to be upwards through the head of a team/department → CIO/COO/CRO or equivalent → to CEO or Board of Directors (generally on a case-by-case basis). In a few specific cases, a specialist committee/board had been set up (which includes the CEO) to handle critical security issues such as cyber-crime. Only in three cases was it indicated that no formal upward reporting arrangement exists.

Figure 6: Is the cyber threat generally discussed and understood by senior management?



Cyber-crime and cyber security is also defined and captured in formal documentation and plans, suggesting some level of 'embeddedness'. Most exchanges surveyed (89%) report having a formal plan/documentation addressing cyber-attacks or cyber-threats and over two-thirds have a definition or use an existing definition of cyber-attacks or cyber threats internally (see Figure 7, 8).

Figure 7: Does your organization have an internal definition or use an existing definition relating specifically to cyber-attacks or cyber threats?

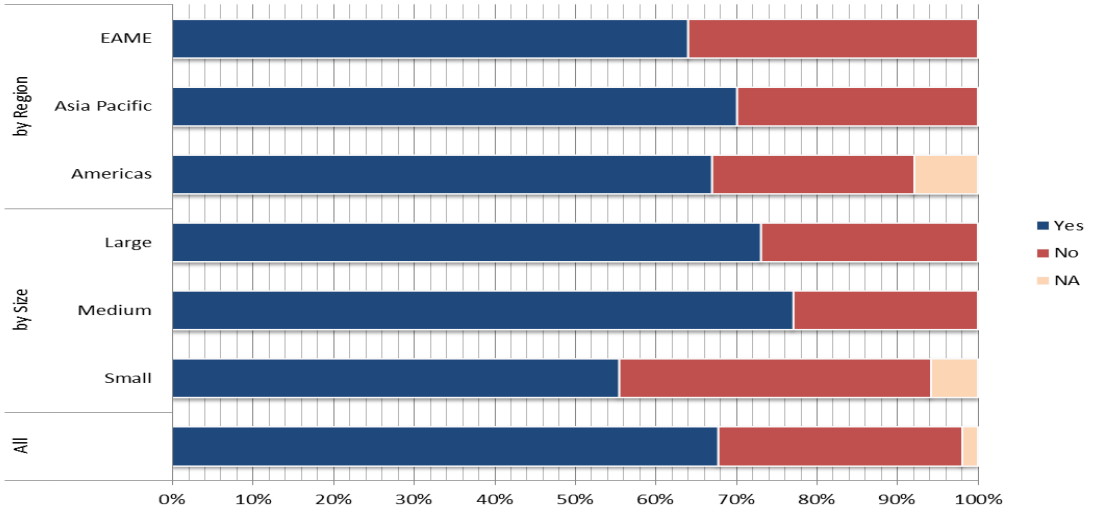
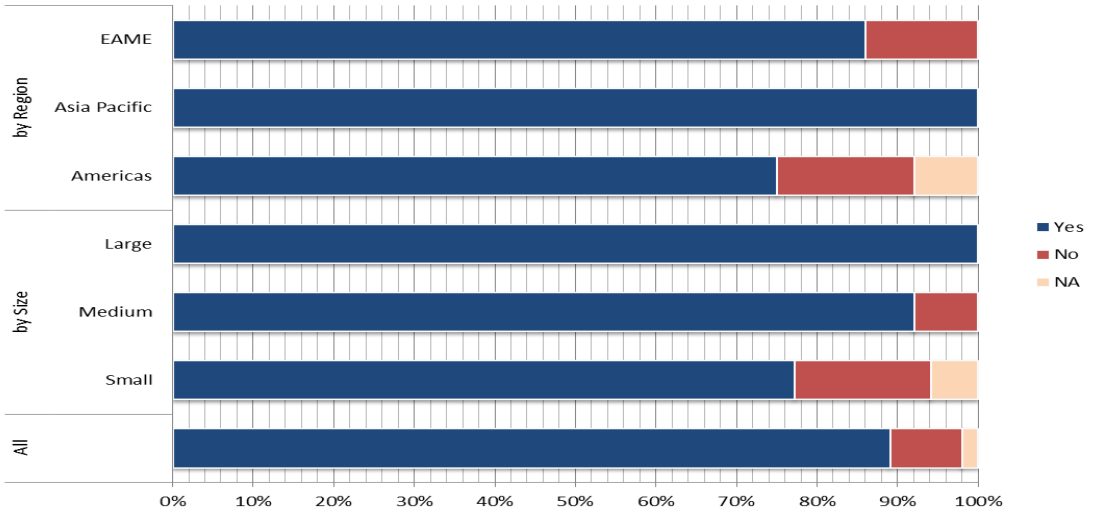


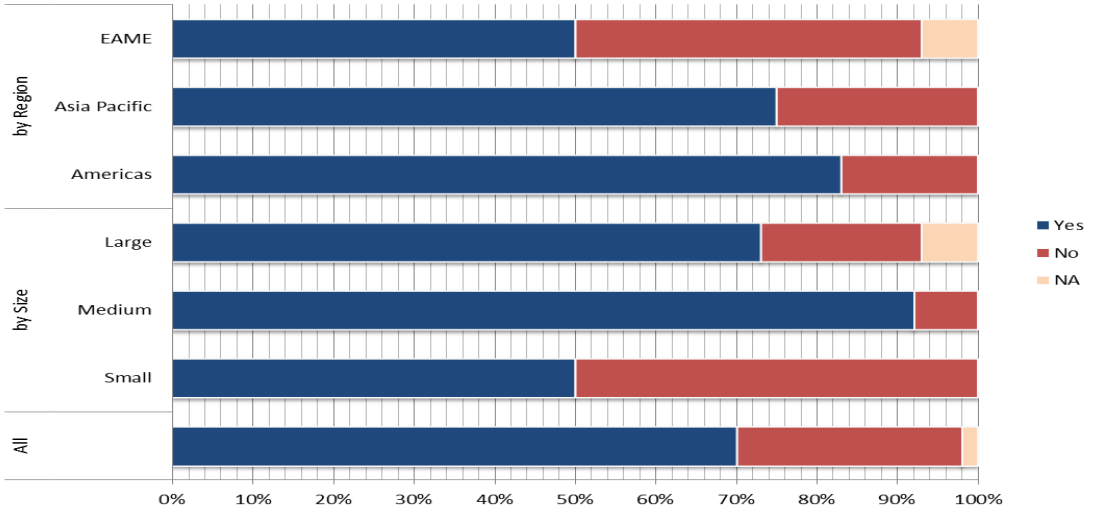
Figure 8: Does your organization have any formal plan or documentation addressing cyber-attacks or cyber-threats?



Plans included: General information security plans, Security incident response procedures, incident handling, scenario planning, crisis management and recovery plans, documentation on types of threats/attacks, business plan for cyber-attack prevention, addressed in business continuity plans, specific plans moulded on threats e.g. Denial of Service attack plans.

Information sharing arrangements are used, but most are not cross-jurisdictional in nature. 70% of exchanges surveyed (72% of larger exchanges and 92% of medium exchanges) report that they share information on attempted or successful cyber-attacks with authorities, overseers or regulators (Figure 9). Most report to *national* authorities, regulators and *nationally* focused cyber-threat forums with limited or no cross-jurisdictional information sharing arrangements in place. At the same time, respondent exchanges from all regions take advantage of vendors, online forums, news articles and security reports to glean information of emerging threats. These sources, while not formalized, tend to be more international in nature.

Figure 9: Do you share information on attempted or successful cyber-attacks (e.g. figures and statistics) with authorities, overseers or regulators?



Information sharing arrangement of smaller exchanges varies considerably and includes: sharing with auditors or relevant regulator (including securities regulators); information exchange with brokers, custodians and listed companies; a national forum for combatting cyber-crime and a national scientific research organisation; to SROs and authorities; mandatory sharing through private-public partnerships; and with customers affected.

For medium sized exchanges, information sharing tends to involve sharing with securities regulator, national security council or other supervisory authority; mandatory sharing through private-public partnerships or a dedicated centre.

For larger exchanges, most information arrangements hinge on mandatory sharing through private-public partnership arrangements and dedicated centres; Police; regulatory authorities and government ministries also featured.

♦ *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 (see Figure 10) – however smaller exchanges were less likely to report providing it (72%). By region, 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.[123]

For more than two thirds of respondents providing training, training is repeated at least once a year (see Figure 11). Types of training reported included: awareness training for business continuity and IT security; Information Security Awareness programs; provision of information on most common forms of cyber-attacks; monthly newsletter updates, emails or bulletin boards; computer training modules and quizzes; internal/external table-top exercises.

[123] Almost all exchanges in the Asia Pacific region offer general staff training (95%). The same may be true of the Americas however only 83% of respondents from that region answered this question (all affirmatively).

Figure 10: Does your organization have cyber security related staff training for general staff?

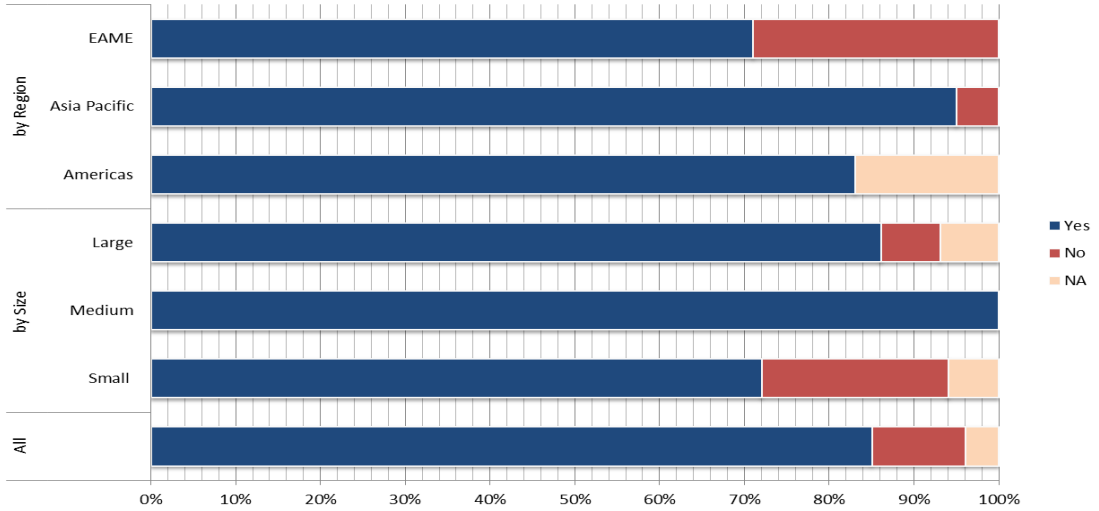
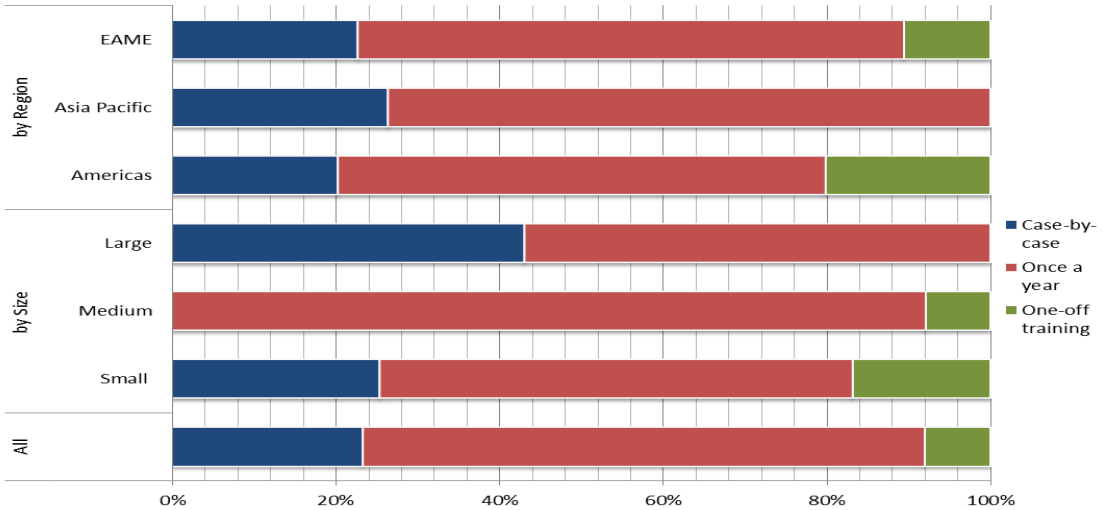


Figure 11: How often is this training repeated?

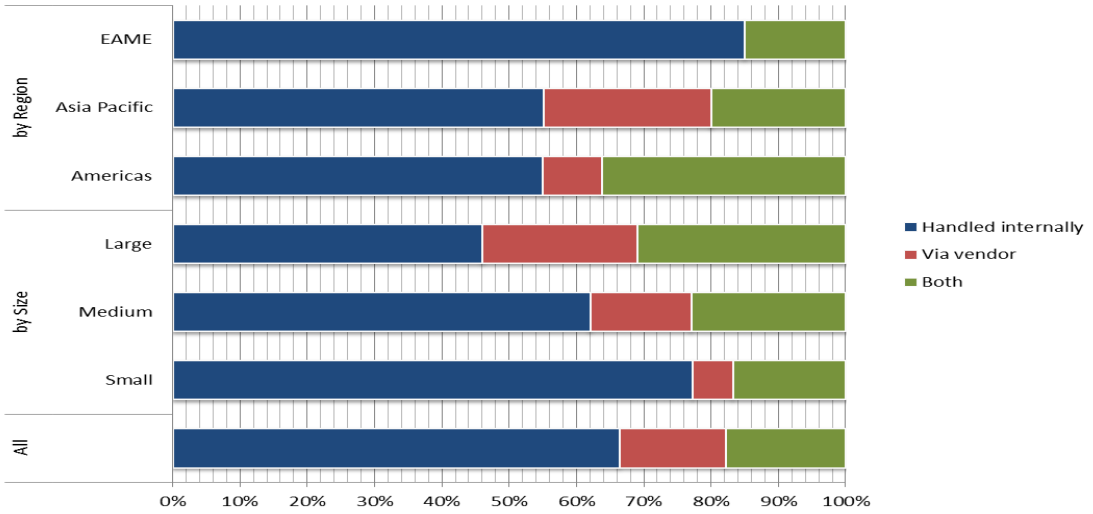


Cyber-attacks against respondent exchanges are generally detected immediately however some respondents noted that detection times may lengthen when facing 'zero day' or unknown threats. Nearly all exchanges surveyed state that the most common and most disruptive cyber-attacks are generally detected immediately (within 48 hours). It is worth noting however that one of the most common forms of attack experienced by exchanges ('Denial of Service' attacks) are designed to have immediate and observable impacts, heightening chances of quick detection. Future threats may not follow such predictable patterns (so-called 'zero day' threats).

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: Internal detection systems are valuable in identifying anomalies specific to a particular entity's system and infrastructure whereas external event monitoring, via a vendor, is also useful in detecting new threats as they emerge across a range

of actors. All exchanges surveyed have some form of detection system in place, however only 32% of exchanges reported utilizing both internal and external event monitoring via a vendor.

Figure 12: Is Information Security Event monitoring handled internally or via an external vendor?



Preventative and disaster recovery measures are in place but a number of exchanges recognize that due to the severity of the threat, 100% security can never be ensured. According to responses to the WFE/IOSCO survey, all exchanges employ a number of preventative and detection mechanisms (see Annex B for examples). There are also a few specific mentions of scenario planning and 'risk registers' – which constitute more proactive defenses. Furthermore, nearly all (94%) of exchanges surveyed report that disaster recovery protocols are in place in their organization (see Figure 14).

At the same time, almost one quarter of exchanges surveyed note that current preventative and recovery mechanisms may not be sufficient in the face of a large-scale, coordinated cyber-attack, especially given the rapid innovation of the cyber-threat and growing capabilities and resources of cyber-criminals. As such, given the severity and evolving nature of the threat, 100% security and resilience of an entity cannot be ensured and system-wide preventative and resiliency measures may need to be utilized.

Figure 13: Would you consider the preventative measures currently employed by your organization as sufficient in the face of a coordinated, large-scale cyber-attack?

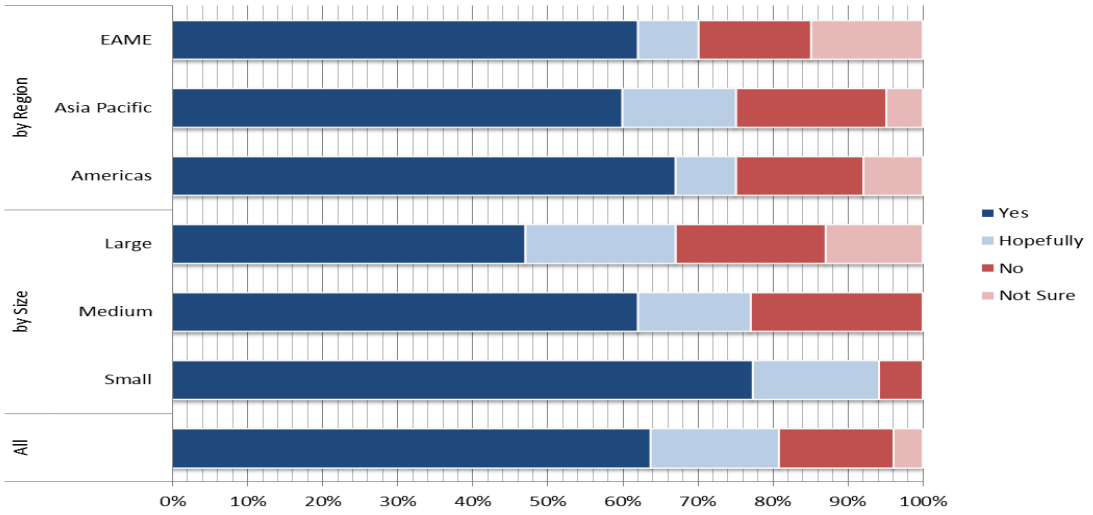


Figure 14: Are disaster recovery protocols/measures in place?

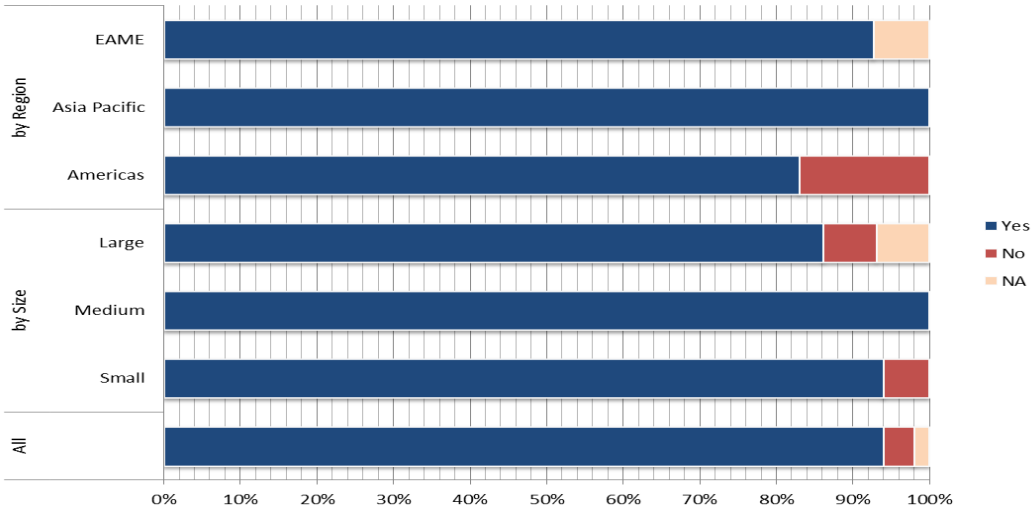
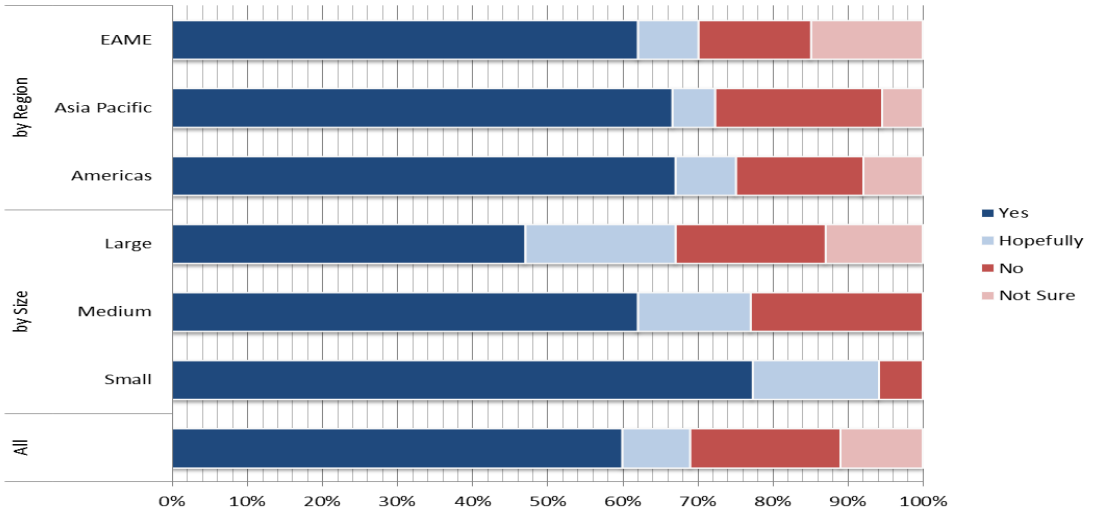


Figure 15: Would you consider the disaster recovery protocols currently in place you your organization as sufficient in the face of a coordinated, large-scale cyber-attack?

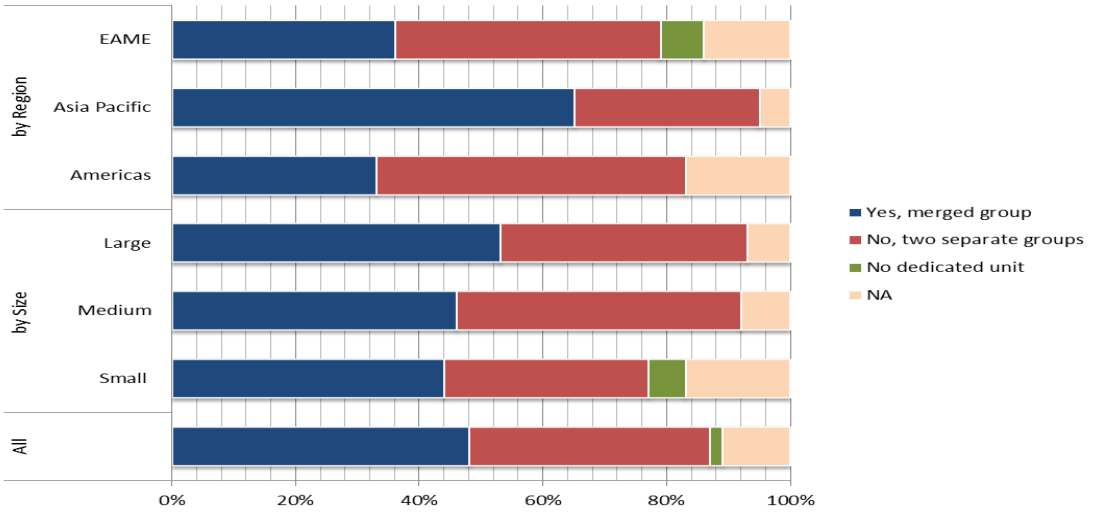


Around half of exchanges report having separate cyber and physical security teams, which could pose a challenge in engaging with cyber-physical threats, in the absence of relevant coordination between the two groups. The physical and cyber world are not completely separable.[124] Yet physical and cyber security have traditionally been treated as separate disciplines. Recently, this has changed with the realisation that silo-ing both security areas can lead to vulnerabilities, especially when it comes to dealing with cyber-physical security threats.[125] In the WFE/IOSCO survey (see Figure 16), a number of exchanges (around half) report having separate groups to handle physical and cyber security. While separation of the two teams could lead to challenges in engaging with cyber-physical threats, these challenges may be easily overcome (if not already) through efficient and on-going coordination between the two groups. Further information around the level of coordination between these two groups could shed light on this point.

[124] Cyber Threat Intelligence Coordinating Group, Multi-State Information Sharing & Analysis Centre (MS-ISAC), "Building a Communication Bridge Between Cyber and Physical Security

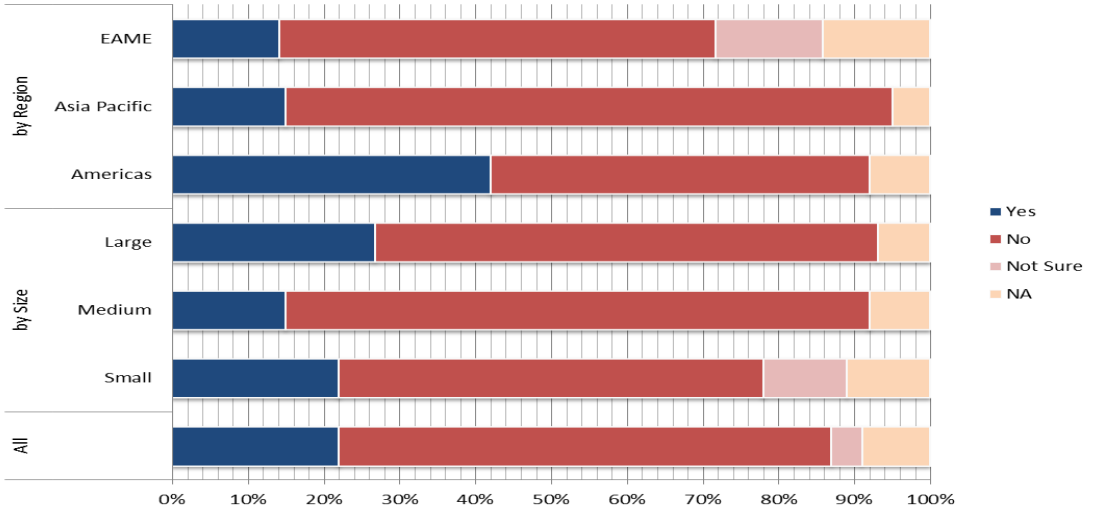
[125] James Willison, The Blended Threat of Cyber & Physical Security, IFSECGlobal.com, http://www.ifsecglobal.com/author.asp?section_id=541&doc_id=559382&cid=ifsecglobal_sitedefault

Figure 16: Does your organization have a merged group that handles both information security and physical security threats?



Due in part to unavailability and relevance, cyber-crime insurance is not yet widespread. 22% of respondents have cyber-crime insurance or something similar, with exchanges from the Americas are more likely to have it (42%) (see Figure 17). For those that do not, a number of reasons were provided – insurance is: not available, cost-prohibitive; has significant coverage limitations (e.g. reputational damage not considered); or that it is still under consideration.

Figure 17: Does your organization have cyber-crime insurance or something similar?



♦ *Theme 5: Effectiveness of existing regulation*

Existing regulation is not widespread and views are split on the effectiveness of current sanction regimes in deterring cyber-crime. Only 59% of exchanges surveyed report sanction regime being in place for cyber-crime, in their jurisdiction (see Figure 18). Of these, only half (55%) suggest that current sanction regimes are effective in deterring cyber-criminals (see Figure 19). Geographically, the majority of exchanges in the Asia Pacific region which report sanctions regimes in place believe they are effective. Whereas in the Americas and EAME

region, views on effectiveness are much lower (29% and 36% respectively). Doubt over the effectiveness of these regimes generally appears to rest on the international nature of cyber-crime which creates a major obstacle in effective enforcement. This may suggest that, at present, 'a doctrine of deterrence'[126] may be ineffective against the growing threat of cyber-crime, since the likelihood of being caught and then prosecution is low.

Figure 18: Are sanctions regimes in place?

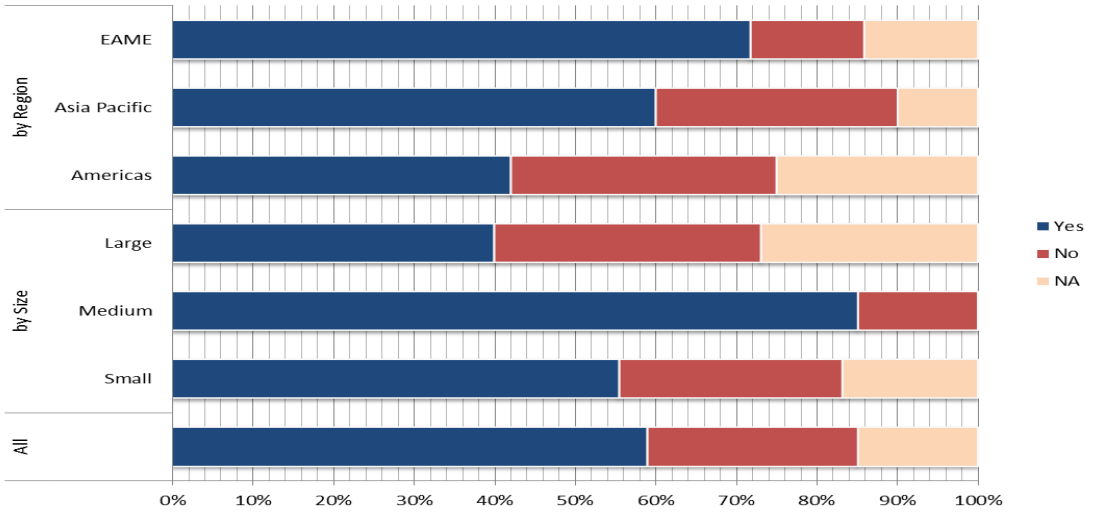
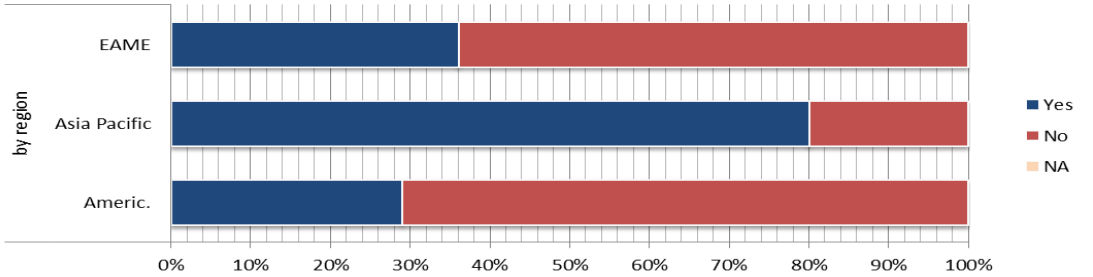


Figure 19: Are they effective in deterring cyber-criminals?



Conclusion: Could cyber-crime in securities markets be a systemic risk?

A **majority of exchanges (89%) view cyber-crime in securities markets as a potential systemic risk,** citing the possibility of massive financial and reputational impact; loss of confidence; effect on market availability and integrity; the interconnectedness and dependencies in securities markets; and related knock-on effects on market participants from an attack (see Figure 20). Analysis around the factors posed in Chapter 1 is in line with this view:

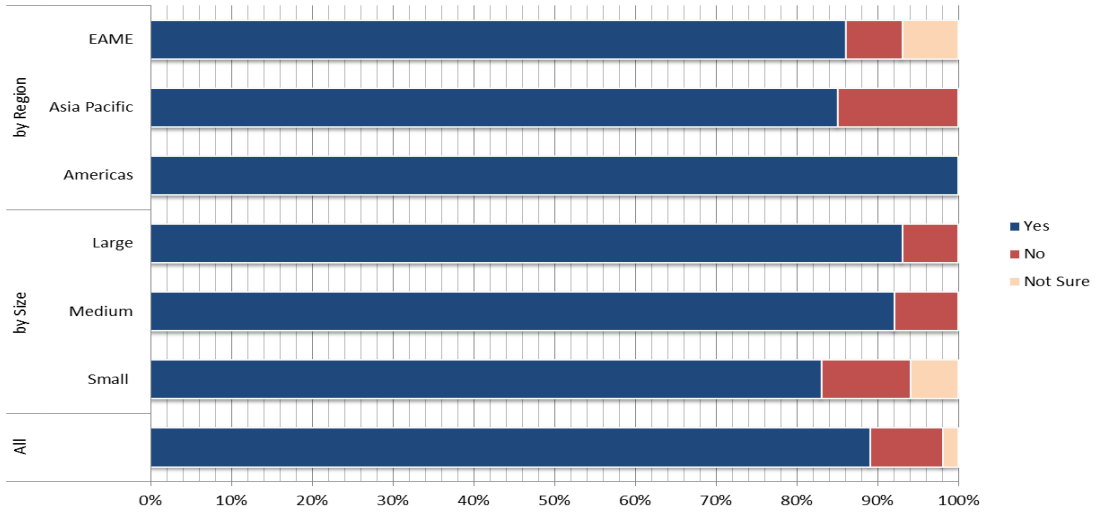
- Cyber-criminals now include sophisticated and well-resourced actors, undeterred by regulation (given the low likelihood of being caught). These actors are perpetrating attacks against securities markets with the motive of being disruptive and not just for immediate financial gain. The most common forms of attacks against exchanges are disruptive in nature - separating cyber-crime from traditional financial crime such as fraud and theft.

[126] Peter Sommer, Ian Brown, 'Reducing Systemic Cybersecurity Risk', OECD, 2011, OECD/IFP Project on 'Future Global shocks',

- Disruptive future attacks could potentially affect market integrity and efficiency (e.g. taking down critical systems, manipulating information, moving markets through unauthorized access). If attacking a number of interconnected providers of essential and non-substitutable services, impacts of the attack could have knock-on effects to other market actors. Future costs could be borne mostly by the victim institution since cyber-crime insurance is not yet widespread.
- While detection for cyber-attacks is immediate and impacts have been minimal so far, 100% cyber-security is illusionary and current preventative and disaster recovery measures may not be able to withstand all 'zero-day', coordinated and large-scale attacks in the future. An attack following an unknown pattern could infiltrate undetected for a long period, especially if tailored for the victim institution(s) – as general information providers such as vendors, security specialists and the media may not know of it in time.
- By targeting exchanges in different parts of the world, existing information sharing arrangements may not be enough to facilitate fast communication of an emerging threat or the mounting of a cross-border response. Furthermore, attacks could take advantage of weaknesses in both the cyber and physical world if there is not effective coordination between cyber and physical security teams.

As such, further consideration and engagement of cyber-crime in securities markets as a potential systemic risk appears warranted.

Figure 20: Should cyber-crime be considered as a potential systemic risk?



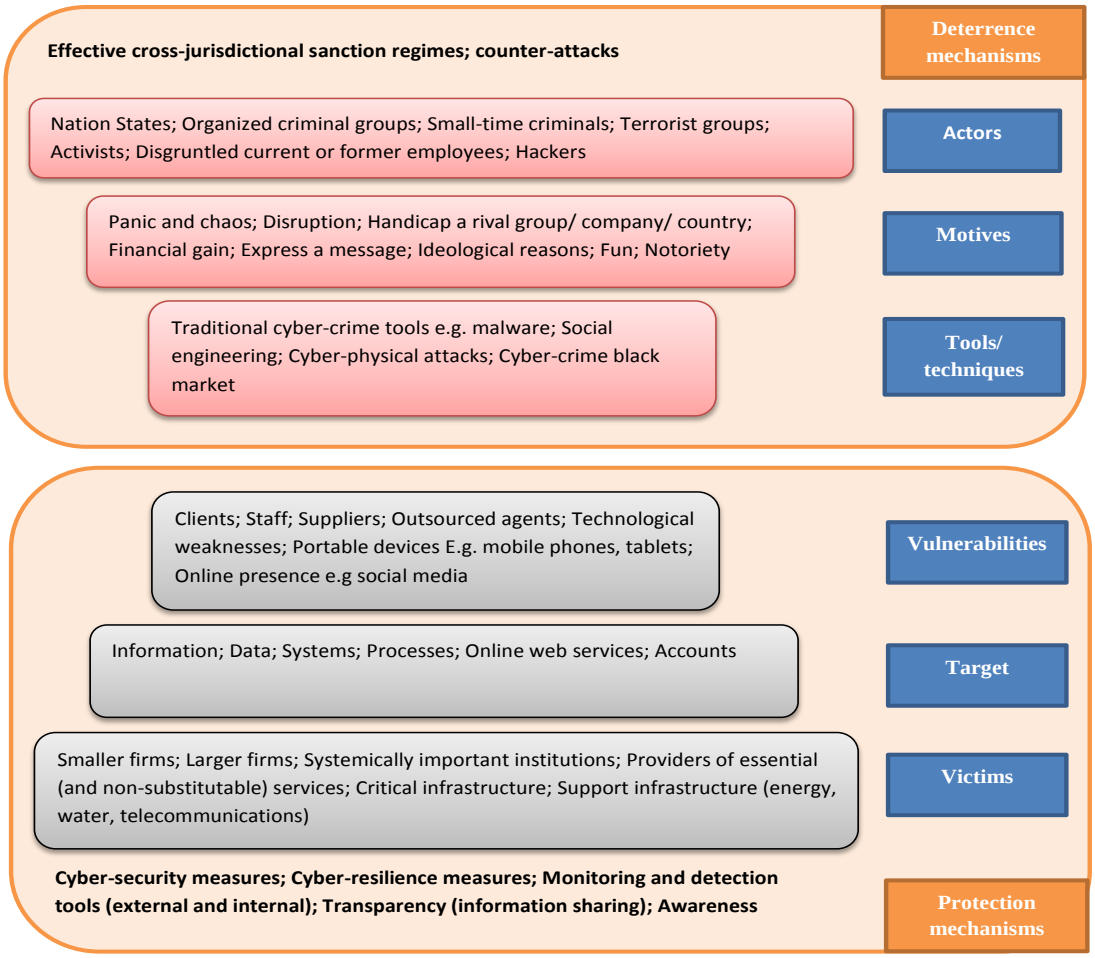
Response excerpts:

- *"In the hypothesis of a successful attack to our post-trading platform, lack of liquidity risk controls combined with absence of a CCP within the time frame of the settlement window may lead to systemic risk."*
- *"It is a matter of degree - some cyber-attacks may present a potential systemic risk and some may not. Our infrastructure, and that of the entire financial services industry, is heavily electronic, very interconnected, and highly correlated. Accordingly, a successful cyber-attack targeting even an isolated environment could have the potential to have far reaching effects on global financial markets. However, not all cyber-attacks are equal. For example, an attack targeting specific intellectual property (through an Advanced Persistent Threat or some other means of cyber-attack), while a serious issue, would be typically isolated enough to not present a risk to the larger financial system."*

- *"The wave of APT last year proved that adversaries may not have direct access to core systems, but by burrowing into internal systems, they gain line of sight indirectly."*
- *"It should be considered a potential risk if left unmitigated / untreated over a prolonged period of time, and persistent cyber-attacks such as DDOS or APT can cripple our financial market by bringing our IT infrastructure systems to a standstill."*
- *"Since the technology is developing swiftly, it is hard to prevent cyber-attacks thoroughly. If the aim of cyber-attacks is achieved, it may cause huge impact on the market fairness and stability."*

Cyber-crime in securities markets has not manifested systemic impacts at this stage, but the analysis of this report suggests there is potential for it to. Cyber-crime is rapidly evolving in terms of its reach, its form, the types of actors, motives and supporting structures; the increasing complexity, sophistication and frequency of attacks; and the number of high-profile cases in different sectors (see Diagram 2). This means that the full nature and extent of the threat is difficult to comprehensively and authoritatively pinpoint at any one point in time.

Diagram 2: The nature of cyber-crime in the financial system



Reliance on an out-dated understanding of what cyber-crime entails; a perception of safety due to containment of past cyber-attacks; or assumptions around the limited capabilities of cyber-criminals *today* – may mean we end up "bringing a knife to a gun fight" in the *future*.[127] Worse, a presumption of safety (despite the reach and size of the threat) could open securities markets to a cyber 'black swan' event.[128]

[127] Radware, 'Global Application & Network: Security Report', 2012.

[128] A black swan event is a concept introduced by Nassim Nicholas Taleb in his book 'Fooled by Randomness' (2001). The term refers to an event which is rare (an outlier), has extreme impact and is predictable in terms of its impact only after the fact.

Cyber War, a controversial book by Richard Clarke, former U.S. White House staffer in charge of counter-terrorism and cyber-security, fleshes out the impacts of such an event in a worst-case-scenario where the world's critical infrastructure is catastrophically compromised. In the book, military and satellite communications are brought down, explosions are triggered at oil refineries, chemical plants and pipelines, air-traffic, metro and freight systems collapse, financial data is deleted and back-up systems wiped out and the electricity grid shuts down.[129]

Clarke posits that "*a sophisticated cyber war attack by one of several nation-states could do [this] today, in fifteen minutes*." He also warns, "*Even though historians and national security officials know that there are numerous precedents for institutions thinking their communications are secure when they are not, there is still resistance to believing that it may be happening now, and to us*." Even though Clarke's scenario is labelled as alarmist by some,[130] it is possible that we cannot fathom the full extent of the costs of cyber-crime until we witness 'a catastrophic cyber event' – and by then it may be too late to appropriately engage with the threat and mitigate damage.[131] It is therefore prudent to consider steps towards mitigating the risk during 'peace-time'.[132] [133]

Identifying the gaps

As highlighted in this report, the full extent of the cyber-threat in securities markets and potential for damage is not, and perhaps cannot be, known. One way to overcome this uncertainty and still engage with cyber-crime is to envision and list potential factors and scenarios where cyber-crime *could* have the most devastating impacts and then mould responses to best engage with those factors, effectively minimizing opportunities for cyber-attacks to manifest systemic consequences.

This report has provided one framework of factors and indicators that could assist in such an exercise. The analysis for exchanges suggests:

- Cyber-crime is already infiltrating securities markets' core infrastructure and providers of essential (and non-substitutable services);
- it is affecting numerous targets around the world (more than half of respondent exchanges);

[129] Richard A. Clarke, Cyber War: The Next Threat to National Security and What to Do About It, 2010

[130] See Peter Sommer, Ian Brown, Reducing Systemic Cybersecurity Risk, OECD, January 2011; also Howard Schmidt, U.S. President Barack Obama's former advisor, stated "there is no cyberwar" in a 2010 interview with *wired* and continues to warn against hyperbolic framings of the threat; and Jami Shea, Deputy Assistant Secretary General, Emerging Security Challenges, NATO commented that *"we must* distinguish between cyber as a problem and over-hyped scenarios like cyber "Pearl Harbors" or a "Cybergeddon". There is no evidence to date that a country can be durably paralysed by cyber-attacks or can lose a war wholly in cyber-space.
[http://www.europesworld.org/NewEnglish/Home_old/Article/tabid/191/ArticleType/ArticleView/ArticleID/21940/language/en-US/Default.aspx]

[131] Janet Napolitano, Head of U.S. Department of Homeland security stated "We shouldn't wait until there is a 9/11 in the cyber world…There are things we can and should be doing right now that, if not prevent, would mitigate the extent of damage."; U.S. President Barack Obama put forward in his State of the Union Address "America must also face the rapidly growing threat from cyber-attacks… We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."; Leon Panetta, U.S. Defense Secretary, stated ""The whole point of this is that we simply don't just sit back and wait for a goddamn crisis to happen." Also see KPMG, 'Shifting View', 2012
http://www.kpmg.com/TT/en/IssuesAndInsights/ArticlesPublications/Documents/Nuanced-Perspective-on-Cybercrime-Art.pdf

[132] *For example Jami Shea, Deputy Assistant Secretary General, Emerging Security Challenges, NATO [http://www.europesworld.org/NewEnglish/Home_old/Article/tabid/191/ArticleType/ArticleView/ArticleID/21940/language/en-US/Default.aspx]*

[133] KPMG, 'Shifting View', 2012

- it tends to be disruptive in nature although more information is needed on the complexity of attacks;
- While it has not yet impacted market integrity and efficiency, a large-scale, successful attack may have the potential to;
- There is a high level of awareness of the threat within exchanges but there may still be gaps in terms of resourcing and engaging with cyber-physical threats.
- Cyber-security and cyber-resilience measures may not be enough, in the face of a large-scale, coordinated attack;
- Information sharing is occurring widely, however there is a lack of formal cross-jurisdictional information sharing arrangements, making it difficult to paint a full picture of the threat landscape and quickly identify emerging cyber-risks before it's too late;
- Current regulation may also not be effective in deterring cyber-criminals from damaging markets since the global nature of the crime makes it difficult to identify and prosecute them.

From this summary, at least four potential gaps in current efforts to engage with the threat can be discerned, in terms of:

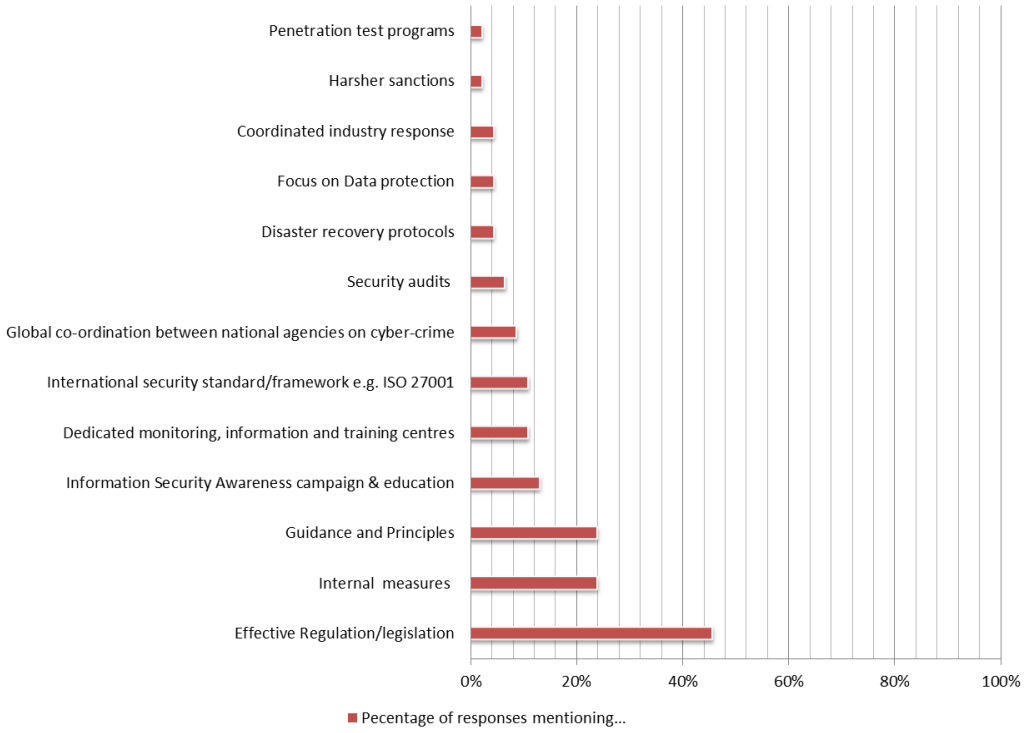
1. Cyber-security and cyber-resilience measures across actors;
2. Cross-border cooperation
3. Transparency of the threat landscape;
4. Regulation for deterring cyber-criminals.

Engaging with the risk - a role for securities market regulators?

Respondents to the WFE/IOSCO survey provide insight on a number of general policy tools and measures that would help their organization better address the aforementioned gaps by ensuring (see Figure 24):

- **The strengthening of cyber-security and cyber-resilience measures across actors** e.g. through guidance and principles, internal measures and international security standards/frameworks.
- **Improving transparency of the threat landscape** e.g. information sharing, dedicated monitoring, information and training centres, information security awareness campaign and education.
- **More effective regulation for deterring cyber-criminals** e.g. through updating/implementing regulation.

Figure 24: Policy tools you believe would help your organization in better addressing cyber crime

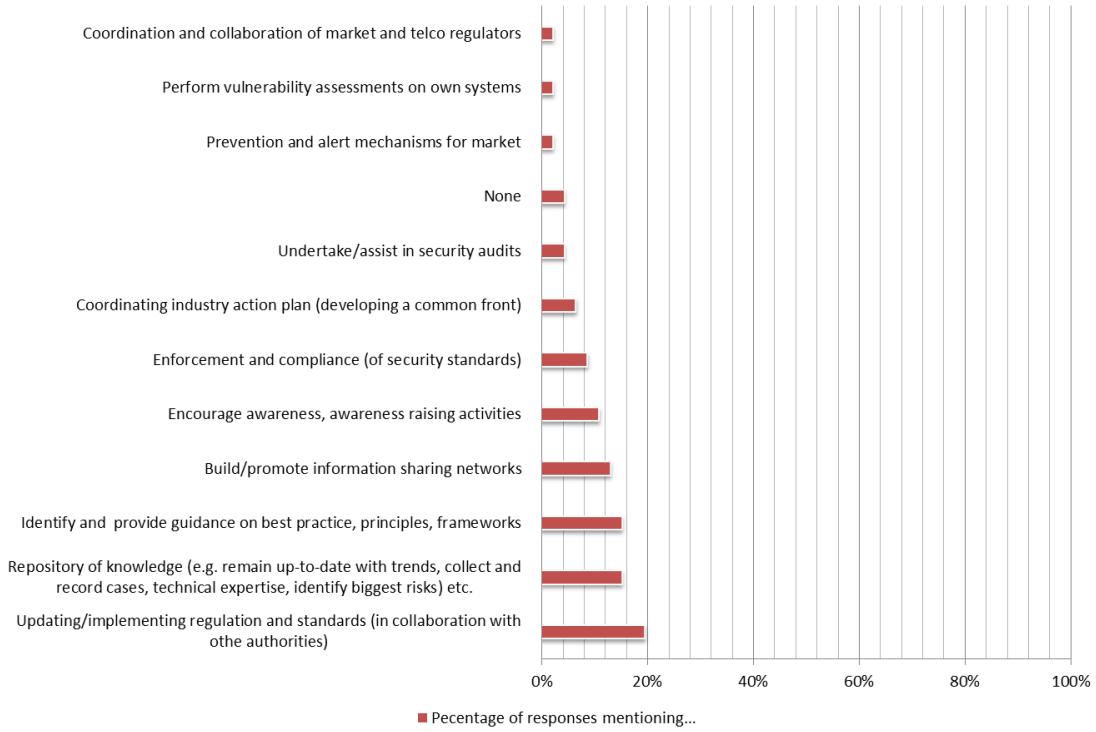


In terms of a specific role for securities market regulators, respondents noted that any regulatory response should avoid being prescriptive; maintain flexibility to adapt to changing threats; concentrate on collaboration; and avoid interference with an institution's own tailored internal measures or policy. Specific activities highlighted included (see Figure 25):

1. **Updating/implementing regulation and standards** (in collaboration with other authorities);
2. **Identifying and providing guidance on best practice**, principles and/or frameworks for cyber-security and cyber-resilience;
3. Building, partaking in and promoting **information sharing networks**;
4. Acting as a **repository of knowledge for securities market participants** to tap into (e.g. keep up to date with trends, house technical expertise to answer industry questions, collect and record cases, identify biggest risks).

.

Figure 25: What do you see as the role for securities market regulators in this space?



Other policy questions for reflection

- ***Emergency planning.*** In the case of a large-scale and debilitating attack on securities markets, a number of questions around 'clean-up' and 'recovery' arise:
    - If a catastrophic attack against a private firm is done as 'an act of war' against a nation state, which body is responsible for bearing the costs?
    - If the institution faces bankruptcy, will another form of government bail-out be required to maintain financial stability?
    - If so, could this introduce moral hazard in terms of private investment in preventative and recovery tools - especially if "the costs of that [investment] decision fall mainly on others"?[134]
    - Is cyber-crime insurance effective and how is it pricing the risk?
    - Is there a role for securities regulators and/or IOSCO in facilitating cross-border emergency planning and public communication of attacks?
- ***Enhancing cooperation and facilitating cross-border sanction regimes.***
    - Could tools such as the IOSCO MMoU and alert system be harnessed by IOSCO members to increase mutual cooperation in identifying cyber-crime risks and prosecuting cross-border cyber-crime in securities markets?

[134] Peter Sommer, Ian Brown, 'Reducing Systemic Cybersecurity Risk', *OECD,* 2011, OECD/IFP Project on 'Future Global shocks',

- Could IOSCO act as a forum for providing harmonized and clear guidance on regulation concerning counter-attacks?

- ***Education and Training.***
    - Could IOSCO develop awareness, education and training initiatives on cyber-crime for emerging and developed securities markets, through the IOSCO Foundation?

- ***Guidance and Principles.***
    - To what extent does current guidance and principles e.g. the CPSS/IOSCO Principles for Financial Market Infrastructures, deal with the threat of cyber-crime. Is coverage sufficient?

Further research questions to consider

The cyber-crime risk has many faces: it is a "technical issue, economic risk [and] security threat".[135] This raises number of challenges around engaging with cyber-crime, from a systemic risk perspective. Future research could thus consider the following questions:

- ***Is cyber-crime against other securities market actors a systemic risk?*** Further research could apply the framework of factors and indicators introduced in this report to a number of different groups in securities markets, to deepen understanding around cyber-crime and the potential for systemic risk.
- ***What further indicators could be developed to better track cyber-crime trends in securities markets?*** The indicators posed in this paper could be used as a starting point for monitoring efforts. Further research could attempt to add and refine the list.
- ***Can cyber-crime be effectively deterred or only defended against?*** A notable study on cyber-crime posits that "we should spend less in anticipation of cybercrime (on antivirus, firewalls, etc.) and more in response (that is, on the prosaic business of hunting down cyber-criminals and throwing them in jail)".[136] However, such a response only works in mitigating potential systemic risk if we assume that cyber-criminals can in fact be deterred. Can they?
- ***What about the social, behavioural and political dimension?*** Cyber-crime is a technology-based risk, however cyber-crime in securities markets is not simply an 'IT' issue[137] nor will a purely technological solution suffice. Further research could attempt to identify how culture, behaviour and political relationships could intensify or reduce the risk. [138]

[135] Lior Tabansky, "Critical Infrastructure Protection against Cyber Threats", *Military and Strategic Affairs,* Vol 3, no. 2, Nov 2011
[136] "Measuring the Cost of Cybercrime", Ross Anderson, Chris Barton, Rainer Bohne, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore, Stefan Savage, 2012
[137] Lior Tabansky, "Critical Infrastructure Protection against Cyber Threats", *Military and Strategic Affairs,* Vol 3, no. 2, Nov 2011
[138] Peter Sommer, Ian Brown, 'Reducing Systemic Cybersecurity Risk', *OECD,* 2011, OECD/IFP Project on 'Future Global shocks',

Annex A: Cyber-attack techniques

The following table lists and categorizes some common types of cyber-attack techniques:

Table 1

Technique	Description	Information Security Issue
Cracking	Cracking involves gaining access to a computer system i.e. through cracking a password.	Confidentiality
Key logging	Device or software that records keystrokes made by the authorized user.	Confidentiality
Electronic funds transfer fraud	Infiltrating the transfer of funds over the internet through diverting them, stealing credit card information etc.	Integrity, Confidentiality
Denial of Service Attacks (DNoS)	Flooding the bandwidth of a website or network with an unmanageable number of information requests, preventing other uses from accessing it or bringing down the server.	Accessibility
Botnet attacks	Compromising of a group of computers by a 'hacker', who then uses the computers to carry out a range of attacks over the internet – spam messages, viruses, DnoS. The authorized user of the computer usually does not know they are part of a botnet.	Confidentiality, Accessibility, Integrity
Hoax email	Phony emails containing an 'alert' about an upcoming threat e.g. a virus, that is quickly passed through a user group by well-meaning individuals and clog up a system.	Integrity, Confidentiality
Malware	Computer code designed with malicious intentions. This can include virus, worm, trojan horse, rootkit, ransomware, scareware, spyware. The most common vessels of infection is through email attachment or the downloading of infected files or application content from websites. A **virus** is a program that attaches to a host files and replicates itself quickly through the system, modifying, deleting or stealing files or causing system crash. A **worm** is similar to a virus but does not require a host file to activate – it will usually spread by sending itself via email to all email contacts. A **trojan horse** appears as a useful or harmless program but provides 'back door' access to your computer. A **rootkit** allows a cyber-criminal to gain access to your system without being detected and install access points in your system that they can be used later. **Ransomware** is similar to a 'worm' – It often restricts access to a computer system and then demands ransom be paid if it is to be removed. Scareware is 'scam software', utilising social engineering to convince users into downloading malicious software e.g. convincing a user that a virus has infected their computer and suggesting the download of (fake) antivirus software. **Spyware** sends personal information from your computer to a third party without your knowledge or consent.	Confidentiality, Accessibility, Integrity
XXS and CSRF attacks	A web application present on a trusted site is presented via hyperlink to an unsuspecting user. Clicking on the hyperlink will download malicious content. CSRF is similar, except a cyber-criminal imitates a trusted user of a site instead.	Confidentiality, Integrity
Pharming	Redirecting users from legitimate websites to fraudulent websites. These fraudulent sites are almost identical to the real ones, however any personal information entered into the forms (password, credit card number etc.) is sent to the cyber-criminal. An attacker can achieve this	Confidentiality, Accessibility, Integrity

	through Domain Name System poisoning.	
Phishing, smishing and vishing	Similar to Pharming, **phishing** also use fraudulent websites to collect confidential information. However a user is first directed to the website through an email appearing to come from a legitimate provider e.g. their bank, urging them to check/confirm their information. The user is than directed to a fraudulent site. **Smishing** is a more sophisticated form of phishing and uses phone text messages to bait victims. **Vishing** aims at tricking a user into making a phone call – either through calling the user or sending them an email. For example, a user may be told that their credit card has been breached ant that they need to call a number to change it. The user rings up the number and enters the credit card number through keystrokes on the phone, which can then be recorded by the cyber-criminal.	Confidentiality, Accessibility, Integrity
Website defacement	Changing the visual appearance and usability of a webpage – usually through breaking into the web server and replacing the original hosted website with a replacement. This is normally done through SQL injections.	Accessibility
Spoofing	Changing the id of a remote computer to the id of a computer with special access privileges on a particular network.	Confidentiality, Integrity
Salami attack	A program that makes micro-changes over an extended period of time, so that the changes are not noticeable e.g. a program that deducts a few dollars from customers of a bank, per month.	Integrity
Misinformation spread	An attack utilizing cyber resources to spread misinformation over the internet and cause panic – e.g. declaring an inevitable bomb attack.	Integrity

Annex B: Prevention, Detection and Recovery mechanisms

Table 2

Reactive defence	Description
Firewalls and antivirus	Firewalls monitor open connections including attachments in an email, block unauthorized/unwanted inbound and outbound internet traffic or connections and disable internet add-ons such as cookies, pop-ups etc. Antivirus software scans any file or data package in your system for viruses (derived from a virus database). They can clean, quarantine and delete any infected files.
Anti-DNoS and Anti-bot detection systems	Software that detects bots and Distributed Denial of Service (DDNoS) attacks and blocks communications.
Intrusion Prevention Systems (IPS) (often combined as Intrusion Detection and Prevention systems).	Software aimed at identifying, logging, reporting and blocking any malicious activity on computer systems. Actions can include e.g. sounding the alarm, resetting connections and blocking traffic from malicious IPs.
Clean Pipe solutions	A 'clean pipe' refers to a communications channel which is cleansed of malicious code or inappropriate content. A user firm will employ the services of a separate company to maintain the security of the channel or 'pipeline'. This separate company will ensure any information passed through the pipeline is devoid of malicious content, before it is passed on to the end-user.
End-point security	Anti-virus software tailored to protect and protect from portable information devices such as USB sticks, smartphones etc. Viruses and malicious content can be transmitted from portable device to computer network and vice versa.
Terminal safety controls	Protection of terminals (e.g. computers) from unauthorized and inappropriate usage. This includes limitation on administrative access, robust authentication systems, centralized logging systems; web browsing and application download controls.
Proactive defence	
Penetration Testing, Ethical hacking and simulations. Regular training exercises on social engineering techniques.	Simulation of an attack on a computer system, to test for vulnerabilities.
Vulnerability assessment	Identification, quantification and prioritisation of vulnerabilities. All potential hazards are assessed and all assets, equipment and infrastructure is catalogued in order to guide prioritization of threats.
Internal and external audits	Continual checks of security controls and systems to ensure they are up-to-date and implemented effectively.
Data encryption	Conversion of plaintext and information into 'cyphertext', which unreadable by anyone else but the intended (who holds a key to decipher it).
Counter attacks	Retributive or mitigative counter strike against cyber-criminal (through hacking back) – to punish for damage or mitigate damage to systems.
Air-gapping or partial air-gapping	Isolating a network from insecure networks such as the internet or local area network, to form a closed and secure system e.g. network zones to isolate critical systems (e.g. with jump servers), closed network for core business and DMZ (or perimeter network).
Detection	

Intrusion Detection Systems (IDS) (often combined as Intrusion Detection and Prevention systems).	Detect hacker attempts and anomalous behaviour e.g. a file integrity checker which detects when a system file has been altered.
Automated Monitoring Systems and outsourcing monitoring (e.g. to CERT specialists)	Automated defence system that allows rapid detection of cyber-attacks and blocking of any follow-up attempts.
Security Incident and Event Management (SIEM) systems for all devices	A 'one stop shop' - Real-time monitoring and analysis of potential security breaches, alerts or unusual activity for all devices (e.g. computers, smartphones). Also reports log data to assist in compliance. Can be used to manage user privileges.
Database activity monitoring	Database security application – monitors and analyses all activity to a database, controls and logs user access and works independent of native database functioning.
Security Operation Centres (SOC)	A centralized unit in an organization that monitors an organization's technological infrastructure and access to this infrastructure.
Disaster recovery	
Back-up systems and data loss prevention software	Automatically detects and secures confidential and critical information and stores on separate systems. Information can be stored and allows restoration in the case of primary system failure.
Redundancy and disaster recovery sites	Storage facilities/data centres located in a separate physical location from the main network.

Annex C: Survey data

1. Does your organisation have an internal definition or use an existing definition relating specifically to cyber-attacks or cyber threats?

	All	By Size			By Region		
		Small	Medium	Large	Americas	Asia Pacific	EAME
Yes	31	10	10	11	8	14	9
No	14	7	3	4	3	6	5
NA	1	1	0	0	12	20	14

2. If yes, what is it?

Not all respondents provided complete definitions, however aspects of cyber-attacks/threats mentioned in responses include (as a percentage of responses):

Refers to information security	39%
Refers to IT incident and IT event	3%
Refers to unauthorized access	10%
Refers to attack on infrastructure, systems or networks	29%
Refers to changes to hardware	3%
Refers to changes to software	3%
Refers to disruption, loss of service or denial of service	10%
Refers to indirect attacks (e.g. attacks on peer institutions)	16%
Refers to social engineering	6%
Refers to an attack on confidentiality, integrity and accessibility	19%
Refers to internal and external threats	3%
Refers to types of attacks	16%
Refer to definition provided through relevant authority or international standard (ISO/IEC 27001)	10%
Refers to possible impacts	3%
Differentiates between attacks with deliberate, malicious intent and accidents	6%
Refers to medium of attack e.g. internet	10%
Refers to perpetrators e.g. hactivists, nations states, organized crime	3%

3. Does your organization have any formal plan or documentation addressing cyber-attacks or cyber-threats?

	All	By Size			By Region		
		Small	Medium	Large	Americas	Asia Pacific	EAME
Yes	41	14	12	15	9	20	12
No	9	3	1	0	2	0	2
NA	2	1	0	0	1	0	0

4. Does your organization train general staff on the topic of cyber-crime?

	All	By Size			By Region		
		Small	Medium	Large	Americas	Asia Pacific	EAME
Yes	39	13	13	13	10	19	10
No	5	4	0	1	0	1	4
NA	2	1	0	1	2	0	0

5. If yes, how often is the training repeated?

	All	By Size			By Region		
		Small	Medium	Large	Americas	Asia Pacific	EAME
Case-by-case	9	3	0	6	2	5	2
Once a year	26	7	11	8	6	14	6
One-off training	3	2	1	0	2	0	1
NA	6	5	0	1	2	1	3

6. Is there a merged group that handles both information security and physical security threats?

	All	By Size			By Region		
		Small	Medium	Large	Americas	Asia Pacific	EAME
Yes, merged group	22	8	6	8	4	13	5
No, two separate groups	18	6	6	6	6	6	6
No dedicated unit	1	1	0	0	0	0	1
NA	5	3	1	1	2	1	2

7. Would you agree that cyber-attacks are an issue discussed and understood by the senior management of your organization?

	All	By Size			By Region		
		Small	Medium	Large	Americas	Asia Pacific	EAME
Yes	43	16	13	14	11	19	13
No	2	1	0	1	0	1	1
NA	1	1	0	0	1	0	0

8. Has your organisation experienced a cyber-attack(s) in the last 12 months?

	All	By Size			By Region		
		Small	Medium	Large	America s	Asia Pacific	EAME
Yes	24	5	7	12	8	11	5
No	20	12	6	2	3	9	8
NA	2	1	0	1	1	0	1

9. What was the most common form of cyber-attack experienced?; What do you consider to be the most hazardous form of cyber-crime to your organization?; What was in your opinion, the most disruptive form of cyber-attack experienced - from an organisational standpoint? (percentage of respondents)

	Most common form	Most disruptive form	Most hazardous form
Denial of Service attack	55%	38%	75%
Data theft	3%	14%	45%
Financial theft	0%	0%	9%
Account takeover/ unauthorized financial transactions	7%	3%	20%
Malicious software (virus)	52%	45%	55%
Insider information theft - including of HFT source code	3%	7%	34%
Other	21%	28%	9%

10. Please briefly describe the impact of the most common form of attack on your organisation (percentage of respondents mentioned…).

No impact because of preventative and detection mechanisms	46%
Minimal performance degradations on Internet connections	8%
Disruption or unavailability of production and/or web services	21%
Interfere with daily operation and take up resources	8%
Reputational impact	8%
Manipulation of public information e.g. mined content available on public websites to create false documents (containing viruses) and send out to distribution lists	4%
Minor information corruption	4%

11. Please briefly describe the impact of the most common form of attack on your organisation.

Not all respondents answered this question. Answers generally reflected the results of Question X. Excerpts:

- *'The impact was in the form of intermittent denial of access to our non-trading related services hosted through Internet such as the Website, which could compromise the reputation and confidence of the services provided by the Exchange.'*
- *'I wouldn't say virus issues have been overly disruptive to date. We have strong controls to prevent and if required manage them, hence disruptions are minimal.'*
- *'Disruption of production services.'*
- *'Reputation and service unavailability to clients.'*
- *'We have not been affected adversely by any successful attacks but it has highlighted the need for preventative measures.'*
- *'Time spent re-training employees and managing Anti-Virus software.'*
- *'Since exchange business operations are not running on Internet, we encounter minimal performance impacts on some of the secondary IT operations.'*
- *'Successfully prevented or blocked [so] the service and production is not affected. If the attack aim was accomplished, the business availability may [have] been affected, the company information may be leaked or [it could have] damaged the fairness and stability of the market.'*

12. What do you consider to be the most hazardous form of cyber-crime to the financial services industry? (percentage of respondents)

Cyber-attack	Most hazardous form
Denial of Service attack	61%
Data theft	50%
Financial theft	45%
Account takeover/ unauthorized financial transactions	50%
Malicious software (virus)	45%
Insider information theft - including of HFT source code	43%
Other, please specify	7%

13. How long does it generally take your organization to identify the most common forms of attacks?

All surveyed answered "Immediate (48 hours)"

14. How long does it generally take your organization to identify the most disruptive attacks?

All surveyed answered "Immediate (48 hours)"

15. What would you estimate as the monetary impact (both direct and indirect) of cyber-attacks to your organization in the last 12 months? (USD)

All the surveyed answered "less than 1 000 000"

16. The last two years?

All the surveyed but one answered "less than 1 000 000"

17. Would you say that your organisation employs preventative measures to counter cyber-related attacks?

All surveyed answered "Yes"

18. List the type of preventative measures your organization employs.

See Annex B

19. What is the total capital expenditures and operating expenses dedicated to information security? (USD)

27 organizations answered this question.

For organizations with annual revenues < 100 million USD:	**No. of respondents**
Less than 250 000 USD	5
between 250 000 and 500 000 USD	5
NA	8
For organizations with annual revenues 100 million USD - 500 million USD:	
Less than 1 500 000 USD	5
between 1 500 000 and 10 000 000 USD	4
NA	4
For organizations with annual revenues > 500 million USD:	
Less than 10 0000 USD	6
10 000 000 or more USD	2
NA	7

20. Is information security event monitoring handled internally or via a vendor (managed security services provider)?

	All	**By Size**			**By Region**		
		Small	**Medium**	**Large**	**Americas**	**Asia Pacific**	**EAME**
Handled internally	29	14	8	6	6	11	11
Via vendor	7	1	2	3	1	5	0
Both	8	3	3	4	4	4	2
NA	2	0	0	2	1	0	1

21. Would you consider the preventative measures currently employed by your organization as sufficient in the face of a coordinated, large-scale cyber-attack?

	All	**By Size**			**By Region**		
		Small	**Medium**	**Large**	**Americas**	**Asia Pacific**	**EAME**
Yes	29	14	8	7	8	12	8
No	7	1	3	3	2	4	2
Hopefully	8	3	2	3	1	3	1
Not Sure	2	0	0	2	1	1	2

22. Does your organisation have in place disaster recovery protocols to follow in the event of a successful cyber-attack?

	All	**By Size**			**By Region**		
		Small	**Medium**	**Large**	**Americas**	**Asia Pacific**	**EAME**
Yes	43	17	13	12	10	20	12
No	2	1	0	1	2	0	0
NA	1	0	0	1	0	0	1

23. Would you consider the disaster recovery protocols currently in place you your organization as sufficient in the face of a coordinated, large-scale cyber-attack?

	All	**By Size**			**By Region**		
		Small	**Medium**	**Large**	**Americas**	**Asia Pacific**	**EAME**
Yes	27	10	8	9	7	14	6
No	9	5	2	2	4	3	2
Hopefully	4	0	1	3	1	3	0
Not Sure	5	3	2	0	0	0	5

24. Does your organization have cyber-attack insurance or something similar?*

	All	By Size			By Region		
		Small	Medium	Large	Americas	Asia Pacific	EAME
Yes	10	4	2	4	5	3	2
No	30	10	10	10	6	16	8
Not Sure	2	2	0	0	0	0	2
NA	4	2	1	1	1	1	2

** 14 respondents indicating no cyber-crime insurance coverage or NA, note that cyber-crime insurance is not available in their jurisdiction.*

25. In your opinion, should cyber-attacks be considered a potential systemic risk?

	All	By Size			By Region		
		Small	Medium	Large	Americas	Asia Pacific	EAME
Yes	41	15	12	14	12	17	12
No	4	2	1	1	0	3	1
Not Sure	1	1	0	0	0	0	1

26. Do you share information on attempted or successful cyber-attacks with authorities, overseers or regulators?

	All	By Size			By Region		
		Small	Medium	Large	Americas	Asia Pacific	EAME
Yes	32	9	12	11	10	15	7
No	13	9	1	3	2	5	6
NA	1	0	0	1	0	0	1

27. Describe any information sharing arrangements that your organization is currently involved in.

Number of responses mentioning the following:

	Americas	Asia Pacific	EAME
Securities Regulator, supervisory authority and/or other dedicated commission*	4	11	3
CERT	0	2	0
Dedicated national centre/forums	7	6	3
Auditors	0	1	0
Police	1	0	0
Peer institutions	1	1	1
Clients	1	0	1

*(e.g. telecommunications, national security)

33. What do you use as a primary source of information about cyber-threats? (e.g. vendor feeds, news articles?)

Americas	Asia Pacific	EAME

- Vendors - Public-private partnerships - Newsletters - Specialized cyber threats websites - ISACA - FS-ISAC, FSSCC, CHEF - - CERT - Regulation - Government Agencies - Third Party Brand Protection	- Vendors - Alert notifications through dedicated Commissions - CERT - Forums and online discussions - IT security training courses - News articles - Security briefings from Government - Newsletters - FS-ISAC - Specialized cyber threats websites - Auditors - From peer group - Securities regulator - Feedbacks from internal system.	- Vendor feeds and news articles. - CERT - News articles - Specialized cyber threats websites and portals - Closed user groups - Reports from security solution providers - Security training courses - Public databases that track information security breaches - Forums and online discussions - From peer group

28. Is there a sanction regime in place in your jurisdiction for dealing with perpetrators of cyber-attacks?

	All	By Size			By Region		
		Small	Medium	Large	Americas	Asia Pacific	EAME
Yes	27	10	11	6	5	12	10
No	12	5	2	5	4	6	2
NA	7	10	15	7	3	2	2

29. (respondents where sanctions regimes in place) Do you believe it is effective in deterring cyber-attacks?

	All	By Region		
		Americas	Asia Pacific	EAME
Yes	59%	2	12	4
No	26%	5	3	7
NA	15%	0	0	0

30. If no, why not?

Excerpts:

- *'No Penalties are often a "slap on the wrist".'*
- *'The anonymous attracts people (domestic and international) to trigger a cyber-attack; moreover, the forgeable electronic evidence catalyzes the existence of attacks. Both features are hard to be regulated by the jurisdiction.'*
- *'Cyber-attacks can be launched from anywhere outside of its jurisdiction.'*
- *'Attacks can be initiated from anywhere, even on a global scale.'*
- *'Judicial authorities are not effective enough'*
- *'It is hard to find the real perpetrators - lack of cross border coordination among law and security departments.'*
- *'Not globally coordinated.'*

31. List of describe the top 3 policy tools you believe would help your organization in better addressing cyber-attacks (percentage of respondents mentioning the following tools in their responses).

Tools mentioned	Percentage of respondents mentioning
Disaster recovery protocols	4%
Effective Regulation/legislation	46%
International security standard/framework e.g. ISO 27001	11%
Focus on Data protection	4%
Information sharing	52%
Strengthening Internal measures	24%

Guidance and Principles	24%
Information Security Awareness campaign & education	13%
Dedicated monitoring, information and training centres	11%
Security audits	7%
Coordinated industry response	4%
Global co-ordination between national agencies on cyber-crime	9%
Harsher sanctions	2%
Penetration test programs	2%

32. What do you see as being the role for securities market regulators in addressing cyber-crime? (percentage of respondents mentioning the following roles in their responses)

Roles mentioned	**Percentage of respondents mentioning**
Prevention and alert mechanisms for market	2%
Encourage awareness, awareness raising activities	10%
Perform vulnerability assessments on own systems	2%
Repository of knowledge (e.g. remain up-to-date with trends, collect and record cases, technical expertise, identify biggest risks) etc.	15%
Enforcement and compliance (of security standards)	8%
Coordination and collaboration of market and telco regulators	2%
Coordinating industry action plan (developing a common front)	6%
Updating/implementing regulation and standards (in collaboration with other authorities)	19%
Identify and provide guidance on best practice, principles, frameworks	15%
Build/promote information sharing networks	13%
Undertake/assist in security audits	4%
None	4%

Annex D: List of Figures