WORLD BANK GROUP
Finance & Markets
Financial Sector Advisory Center (FinSAC)

FinSAC: Cyber- Security/Preparedness Seminar

Summary: Concluding Remarks

F. Montes-Negret, FinSAC, Coordinator

The two-day "Regional Seminar on Cyber- Preparedness" held at the Austrian Federal Ministry of Finance (MoF) on May 18-19, 2015 brought to Vienna 65 Sr. officials from the central banks and supervisory agencies and ministries of finance from the region, as well as international experts from leading consulting firms, international banks, EU institutions (Europol, European Central Bank, European Commission, and the European Banking Authority) and the World Bank. The program (attached) was open by the Mr. Harald Waiglein, Director General of Economic Policy, Austrian Federal Ministry of Finance.

The seminar had three main purposes: (1) **to raise awareness, (**2) **to bring a regional perspective on cyber-security, and** (3) **to address the issue of cyber-threats from a stability perspective:**

(1) Raising awareness regarding the risks, reputational and systemic costs, and the complexity of cyber-risks faced by banks and non-bank financial institutions (NBFIS), calling for action within central banks and regulatory agencies and beyond (governments and other stakeholders) to confront them, starting by examining approaches followed by countries with experience in the field (e.g. UK, USA, or Estonia), that can play a critical role not only in the protection of confidential information, but also in the speed of recovery from attacks;

(2) Bringing a regional perspective on cyber-security from the countries of Europe and Central Asia (ECA) based on a regional survey of 14 countries (based on FinSAC's Working Paper # 2), making clear that no country is immune from cyber-threats and flag two key factors: (a) that security threats do not follow the regulatory perimeter and that protective measures and information about cyber-attacks weakens as long as we move away from IT departments and from central banks; and (b) that we are confronted not only with an IT issue, but a governance issue, which must be dealt by the Board of Directors of banks and NBFIs;

(3) Addressing the issue of cyber- threats from a stability perspective by looking at the importance of protecting key aspects of a countries' financial market infrastructures (FMIs).

Day 1:

In his welcoming remarks, Mr. Waiglein, aptly reminded the audience that one of the most recent banking crisis in an EU country in the region and a run on bank deposits was precipitated by an e-mail sent by one of the parties in a dispute. So in an environment of extreme interconnectedness news disseminate very fast and can cause havoc in a few hours, putting, for justified and unjustified reasons, a party or a banking system at risk. Extreme caution, a quick communication strategy, and rapid response must now characterize the work of bank and other financial regulators.

The following discussion of the paper on "Cyber Security Issues and Options (based on a Survey of 14 European and Central Asian Countries)", started by flagging the evolution of the cyber-threats from the 1980s to the present, with the famous 4-Fs characterizing the evolution of the motivation of the attackers from "Fun, and Fame" to "Funds and Force". The analysis of the answers to the 35

questions pointed to the importance of continuing the good work IT Departments are doing but also increasing the investment in training and education. From an infrastructure perspective the importance of redundant capacity of FMIs, particularly payment systems, was highlighted. However, the answers especially emphasized the governance and cyber-preparedness, including quick and smart communication policies, are key issues. It seems clear from the responses received that risks do not end where the walls of central banks and supervisors end. Although it is important to emphasize cyber-risks as key operational risks for the functioning of a market economy, it is important to step up the collection and exchange of information among multiple stake-holders and the importance of private-public partnerships.

The presentation of Europol highlighted the challenges and achievements as regards law enforcement in the field of cybercrime. Europol expects an increase in the size, scope and sophistication of cyber threats and the emergence of new attack vectors, posing new challenges for law enforcement in the near term (2015-16). Direct attacks against financial institutions will increase and well-structured and globally active Organized Criminal Groups will continue to dominate payment card fraud in the EU.

The International Chamber of Commerce (ICC) informed about the newly issued Cyber Security Guide for Business aimed at making its members (about 6 million) of 90 National Committees aware of the risks and offer them a guide to mitigate their cyber risks. ICC believes that cooperation of businesses and the public sector is essential to mitigate cyber risk in society and that businesses of all sizes need to develop and nurture key organizational capabilities to manage cyber security. The European Commission introduced their proposal for a Directive on Network and Information Security (NIS), which is currently under negotiation between Council, the European Parliament, and the European Commission and will also affect the financial sector. A regulatory initiative, launched in 2013 by the European Commission, contains legal measures and incentives aiming at making the EU's online environment secure and strengthening preparedness, cross-border cooperation and information exchange. The Directive proposes steps to the system operators of critical infrastructures to manage security risks and report serious cyber incidents with significant impact to competent authorities. The International Telecommunication Union (ITU) brought important information of the United Nations' initiatives under implementation. ITU's Global Cybersecurity Agenda (GCA) is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners, and building on existing initiatives to avoid duplicating efforts. GCA builds upon five pillars: Legal Measures, Technical and Procedural Measures, Organizational Structure, Capacity Building, and International Cooperation. Based on these areas the ITU published the Global Cybersecurity Index (GCI), which aims to measure the level of commitment of each nation in cybersecurity. Finally, ITU referred to National Initiatives (NIs) under development.

ITU's global overview was followed by deep-dives into the strategies of two select country cybersecurity strategies, namely Austria and Estonia. Estonia is a highly digitalized economy, in which 99.8% of bank transactions are effected electronically, introduced a national e-ID in 2002, and introduced voting via internet 2005. After falling victim of a major cyber-attack, Estonia introduced a Cyber Security Strategy in 2008, which was refined in 2014. Due to the fact that government services depend heavily on private sector providers, Estonia considers cybersecurity as a joint private and public sector effort.

The discussion moved to what are major international banks and financial infrastructures are doing in this area to confront the challenges. The cases of Citi, CLS Bank International, MasterCard, and EBA Clearing and their diverse sets of risks and responses were discussed in detail (see presentations). EBA Clearing, for example, is considering the introduction of a separate 'cyber resilience framework', which would enable us to create a specific cyber threat model, asses the

current level of cyber resilience of all relevant stakeholders. MasterCard is subject to biannual reviews by the Federal Financial Institution Examination Council (FFIEC) and performs external penetration quarterly.

DAY 2:

The second day emphasizes systemic nature of cyber-threats focusing on the threats to the FMI. One of the many highlights of the second day, was an outstanding panel session led by Mr. Massimo Cirasino, Practice Manager from the World Bank, with three panelists from the European Central Bank, the US Federal Reserve System, and Banca d'Italia in which cyber-threats to FMIs were examined largely from a central banking perspective, focusing on the centralization of risks, the lack of payment alternatives sand the search for systemic solutions to the systemic risks faced. The participants became aware of the CPMI report on Cyber Resilience and detailed aspects, like the importance of maintaining settlement finality, highest reliability in processing, business continuity and fast recovery (aiming for a two-hour recovery after a major successful attack/event), and a resilient market infrastructure (resistant, reliable and flexible with the concept of cyber-agility). One of the participants emphasized the importance of following a zero-trust approach and the importance of simplicity, not fighting the prior war. Cyber-preparedness is a team sport in which cooperation (not trust) are critical.

Cyber-security threats to the financial industry were the topics explored by the speaker from the European Banking Association and UniCredit Bank Austria, in which active defense, communication and training play an important role. The Global LEI Foundation (GLEIF), which serves as the operational arm of the Global Legal Entity Identifier System (GLEIS) and supports on a not-for-profit basis the implementation and use of the Legal Entity Identifier (LEI) for legally distinct entities that engage in financial transactions.

Cryptosense, Cybercrime Research Institute, MWR Infosecurity, and Sicherheitskultur.at provided invaluable practical insights into the nature of attacks and possible mitigation measures. Encryption of messages and transaction plays an increasing role in prevention (Cryptosense), as well as the importance of the penetration studies being undertaken by financial and non-financial institutions. The second day ended with a presentation from the Dutch Bankers Association, emphasizing the importance of banks understanding that they do not compete on security and the importance of various industry task forces to enhance cooperation.

Participants were kind enough to assess the effectiveness and usefulness of the two-day seminar and give us ideas about possible future events of this kind. Based on the evaluation results attendants were highly satisfied with the event (preparation and content delivery was rated 4.8 out of 5, facility 4.9, and speakers 5.0). Two thirds would welcome similar events to take place annually, one third even semi-annually. We hope that the Seminar will help participants in their work and that they took home some new ideas and initiatives about the importance of cyber-preparedness.

FinSAC would like to thank the speakers for their excellent contributions and stands ready to continue supporting country efforts in this important area.