FLORENCE SCHOOL OF BANKING AND FINANCE

ROBERT SCHUMAN CENTRE

Professional Training Course

Cyber Risks and Resilience

@EUI_FBF_School, @EUI_Schuman

20 - 22 June 2022

Sala Europa - Villa Schifanoia, Via Boccaccio 121 - Florence

Format: **Residential**

Course instructors:

- **Emran Islam** | International Monetary Fund
- **Klaus Löber** | European Securities and Markets Authority

Faculty:

- **Constantinos Christoforides** | European Central Bank
- **Robert Dartnall** | Security Alliance
- **Givan Kolster** | Falconforce
- **Alexandra Maniati** | European Banking Federation
- **Elisabeth Noble** | European Banking Authority
- **Lone Natorp** | Danmarks Nationalbank
- **Paul Williams** | Bank of England

Programme

20 June

13:30 - 14:00 *Welcome and presentation of the School followed by a tour de table*

14:00 - 14:45 **Session 1. Cyber threat landscape and outlook** *(Robert Dartnall)*

Security Alliance, a threat intelligence service provider, will present the main developments in the cyber threat landscape, with a focus on the key infrastructures of the European economy, such as telecom, energy, transport and financial market infrastructures

Co-Funded by the Erasmus + Programme of the European Union

14:45 - 15:45 **Session 2. Presentation: Developing and implementing a cyber resilience strategy for the financial sector** *(Emran Islam)*

The financial sector is comprised of different types of entities, ranging from banks to financial market infrastructures to critical service providers. Given the potential impact of a cyber incident on the increasingly interconnected system, it is important that authorities develop and implement cyber resilience strategies for their respective financial sector, encompassing a range of tools and initiatives, in an integrated and holistic manner. This session will provide insight on how authorities can develop and implement such a strategy, and the tools, initiatives and capabilities to deliver it.

15:45 - 16:00 *Coffee break*

16:00 - 17:30 **Session 3. Interactive presentation and classroom discussion: Advancing cyber risk management: from security to resilience – technical training and interactive case studies** *(Emran Islam and Constantinos Christoforides)*

In recent years, regulators have increased their efforts on cyber resilience. The underlying basis for this effort has been the numerous international cybersecurity frameworks. This session will provide an overview of the different approaches taken; an in-depth technical training on the different elements of the frameworks (e.g. Governance, Identification, Protection, Detection, Response and Recovery, Testing, etc); oversight and supervisory approaches and interactive case studies focused on the different elements.

17:30 - 19:00 *Cocktail at Villa Schifanoia*

21 June

9:30 - 11:00 **Session 4 (*continued)* – Interactive presentation and classroom discussion: Advancing cyber risk management: from security to resilience – technical training and interactive case studies** *(Emran Islam and Constantinos Christoforides)*

In recent years, regulators have increased their efforts on cyber resilience. The underlying basis for this effort has been the numerous international cybersecurity frameworks. This session will provide an overview of the different approaches taken; an in-depth technical training on the different elements of the frameworks (e.g. Governance, Identification, Protection, Detection, Response and Recovery, Testing, etc); oversight and supervisory approaches and interactive case studies focused on the different elements.

11:00 - 11:30 *Coffee break*

11:30 - 12:30 **Session 5. Conversation: Can cyber incidents become systemic and what approaches can be taken to address systemic risk?**

Moderator: Klaus Löber

Panelists: Constantinos Christoforides, Alexandra Maniati, Lone Natorp, Paul Williams.

The cyber resilience of a financial entity is in part dependent on that of interconnected banks, FMIs and service providers, as there is a broad range of entry points through which an entity could be compromised. As a result, the interconnectedness of the financial system accentuates the need for strong sector-wide cyber resilience, to ensure that cyber incidents do not become systemic. The core components of effective sector resilience are: market-wide exercises; understanding operational interdependencies through mapping; enhancing crisis management

arrangements; information and intelligence sharing; and cross-border and cross-authority collaboration. This session will be an interactive conversation amongst regulators, addressing the different issues and approaches that authorities can take to manage potential systemic risk.

12:30 - 13:30 *Lunch*

13:30 - 14:30 **Session 6. Cyber testing – Threat intelligence based ethical red-teaming – how and why** *(Emran Islam, Robert Dartnall, Givan Kolster)*

A core part of enhancing the cyber resilience of the financial system is conducting cyber testing. Increasingly around the world, authorities are adopting intelligence-led red team testing frameworks for their financial market. Threat intelligence based ethical red-teaming mimics the tactics, techniques and procedures (TTPs) of real-life threat actors who, on the basis of threat intelligence, are perceived as posing a genuine threat to financial entities. An intelligence-led red team test involves the use of a variety of techniques to simulate an attack on a financial entity's critical functions and underlying systems (i.e. its people, processes and technologies). It helps an entity to assess its protection, detection and response capabilities. An ethical hacker will lead this session, providing insight on such testing and how it is conducted.

14:30 - 14:45 *Coffee break*

14:45 - 16:45 **Session 7. Group activity – Case study: Building a cyber strategy for the financial sector of Wakanda**

Moderators: All faculty members

This session will be an interactive group session, where we will develop a holistic cyber resilience strategy for the financial sector of Wakanda, a fictitious country. The audience will role play as different stakeholders within the country and demonstrate how they can work together to develop and implement a cyber strategy for Wakanda. Course participants will be divided into smaller groups and will work closely with the moderators to develop the strategy.

16:45 - 17:30 **Session 8 (continued). Interactive discussion – Presentation of the cyber strategy for the financial sector of Wakanda**

Moderators: All faculty members

This session will provide the group to present its cyber resilience strategy for the financial sector of Wakanda. This will be an interactive session, where the group will present the strategy to the instructors, who represent the Board of the authorities of Wakanda, and will allow the Board to challenge the group on its ideas.

20:00 - 22:00 *Dinner downtown at L'Osteria di Giovanni*

22 June

09:30 – 10:45 **Session 9. Panel discussion: How to design public-private partnerships – building trust**

Moderator: Klaus Löber

Panelists: Emran Islam, Paul Williams, Lone Natorp, Alexandra Maniati

Given the rapidly evolving threat landscape, and the increased digitalisation and globalisation, there is a real need for all the relevant stakeholders (which include regulators, financial entities and the cybersecurity sector) to establish a forum to exchange ideas at a strategic and Board

level on how best to tackle the new challenges, share best practices and tools, encourage information sharing, and identify gaps and weaknesses in the ecosystem which require collaborative thinking to catalyse effective solutions. This session will be a panel of authorities from different countries that have established and operated such fora to deliver effective solutions for the market.

10:45 - 11:00 *Coffee break*

11:00 - 12:00 **Session 10. Panel discussion: Is Fintech and Innovative technology increasing cyber risk or decreasing it?**

Moderator: Klaus Löber

Panelists: Elisabeth Noble, Givan Kolster, Alexandra Maniati

The rise of FinTechs and other new entrants seeking to shake up markets is causing increased disruption. New technologies, services and ways of working are gaining prominence. Meanwhile increased digitisation and automation can lead to streamlined operations and greater speed. But are these technologies and processes designed and implemented to take into account the cyber threat? Are they mature enough to withstand the increasing cyber threat. This session will be a panel discussion between authorities and industry leads, examining the complex issues around the new landscape.

12:00 – 13:00 **Session 11. Wrap-up**

13:00 - 14:00 *Take-away lunch*