EPFSF Briefing on "Cybersecurity" 19 June 2018

Foreword

It is a remarkable time. New technologies such as Artificial Intelligence, blockchain or the IoT are increasing the opportunities for new user experiences and businesses. However, these opportunities come with challenges that can affect privacy, security and the overall customer trust which is key to the survival of the digital economy.
Some recent examples have shown the devastating effects that cyber attacks can have on businesses (for example through business interruption) and citizens (data loss and trust). They also underline the potential vulnerability of the critical infrastructure to such attacks, undermining the ability of providing critical or essential services. The frequency of cyberattacks is expected to increase in the future, with perpetrators adopting constantly evolving and innovative means of attacking IT infrastructures.

Europe's private and public sectors are increasingly aware of and willing to respond to these threats, and this is no different for the financial sector. Major investments are accordingly being made across these sectors in building their own defences, but also in providing solutions and raising awareness of the need to be prepared.

Cybersecurity is currently high on the agenda of EU and national policymakers, with a range of initiatives being taken to increase the cyber resilience of Europe's financial sector. In May 2017, under the Digital Market Strategy midterm review, the Commission identified cybersecurity as one of its three key priority areas for further EU action in the years to come. In a similar vein, in October 2017, the European Council asked for the adoption of a common approach to EU cybersecurity whilst the European Parliament adopted a non-legislative resolution calling on the EU to invest more in cybersecurity to prevent attacks aimed at critical infrastructure and destabilising societies. The cross-border nature of cyber threats calls for solutions to be developed both at EU and national level and in conjunction with broader initiatives at the G20 such as the work of the G7 Cyber Expert Group.

Current and recent relevant initiatives

In September 2017, following the State of the Union Speech of the Commission's President in which he emphasised the importance of cybersecurity, the European Commission proposed a cybersecurity package. The package aims to update the 2013 EU Cybersecurity Strategy and includes a number of measures aimed at increasing Europe's cyber resilience and joint response across the EU. As a concrete legislative measure, the Commission proposed a "cybersecurity act" to expand the remit of the European Network Information Security Agency (ENISA) to govern a proposed European cybersecurity certification scheme covering products and services, as well as being conferred a permanent mandate as the EU agency for cybersecurity. The package covers other key initiatives such as means to increase information sharing between member state authorities as well as among market players. In addition, a blueprint was recommended to streamline all procedures into one single process and to better define the roles of stakeholders at operational, technical and strategic level should a major cyber-attack or crisis occur affecting multiple member states.

The European Commission's FinTech action plan of March 2018 also focuses on enhancing the security and resilience of the European financial sector, as one of its three primary objectives related to the promotion of technological innovation across Europe. It proposes non-legislative initiatives to further information sharing on cyber threats between financial market

participants and to identify potential solutions while ensuring data protection standards are fully upheld and enforced. It also calls on the European Supervisory Authorities (ESAs) to identify the threats facing the financial sector and assess the need to draw up guidance in this area.

To ensure seamless electronic interaction between businesses, citizens and public authorities, the eIDAS Regulation applies since 2015. It ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available and creates an European internal market for electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication.

In addition, the European Central Bank (ECB) is also taking concrete steps to increase Europe's financial sector resilience to cyber threats:

- In June 2017, after a pilot exercise with major banks, the ECB announced the scheme for reporting significant incidents
- In April 2018, the ECB released a framework on cyber resilience oversight expectations for financial market infrastructures (FMIs). The framework aims to aid FMIs implement the guidance on cyber resilience for FMIs published by the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions (CPMI-IOSCO) in June 2016, and provides overseers with clear expectations to assess FMIs and determine their cyber resilience maturity levels.
- In May 2018, the ECB published a European framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU) to test the resilience of financial market entities considered critical for the functioning of the financial system. The framework aims to harmonise penetration testing across member states to enable mutual recognition of tests and encourage cross-authority collaboration. .

Finally, major steps in information sharing and ability to respond to cyberattacks are being rolled out through the implementation of the Network Information Security (NIS) directive and the General Data Protection Regulation (GDPR) from May 2018.

- The NIS directive sets out a list of sectors that are considered as critical infrastructure or operators of essential services in network security, which includes certain financial services players. The Directive sets out the requirement for the companies under its scope to adopt risk management practices and report major IT security incidents to the competent national authority. The requirement to report IT security incidents aims to help develop a culture of risk management and make sure that information is shared between private and public sectors.
- The GDPR details the general obligations of the controllers and of those processing the personal data on their behalf (processors). These include the obligation to implement appropriate security measures according to the risk involved in the data processing operations they perform. Controllers are also required in certain cases to provide notification of personal data breaches. It provides for very severe sanctions against controllers or processors who violate data protection rules, with fines of up to €20 million or 4% of their global annual turnover.
- The application of both the GDPR and NIS Directive, and the notification requirements within them, will create a wealth of cyber incident-related data that can greatly help understand and prepare for these risks better.

Challenges for the financial sector

Cybersecurity will remain a top priority on the EU agenda and an increasing challenge for both the public and private sectors for the foreseeable future. The financial sector is already taking steps to not only comply with the new and future requirements, but also going beyond to increase its resilience to cyber threats.

However, a coordinated and efficient regulatory/supervisory framework is needed to enable an effective environment for institutions to maximise its cybersecurity resources and continue to manage and improve its cybersecurity programmes.

For example, the banking sector specifically is called to meet multiple incidents reporting requirements provided by both sectorial (PSD2, ECB Target 2 and ECB/SSM) and non-sectorial legislation (e-IDAS, NIS Directive and GDPR).

A single incident might require for a single institution the obligation to report to different Supervisory Authorities respecting the relevant impact assessment details and thresholds, data set, timing, communication means. This creates fragmentation into the overall incident reporting process. The challenge is therefore to streamline as much as possible this overall process as it represents the first crucial step towards an efficient crisis management.

Several initiatives on incident reporting are in place which aim to make authorities aware of the need to harmonize taxonomies and report templates and to implement vertical solutions involving financial institutions, their representative associations and other stakeholders.

Similarly, for wholesale capital markets, firms are increasingly looking at means to harmonise regulatory frameworks and certifications, ensuring a common baseline in the chain to become more efficient in response to cyber threats. Crucial components of a firm's recovery, prevention and preparedness response strategy include risk management and penetration testing frameworks. In addition, wholesale capital markets firms perceive combatting cyberthreats as a shared objective, therefore international cooperation and cross-industry initiatives, in the form of public-private partnerships, are concrete initiatives needed to increase the overall cybersecurity lifecycle of the financial eco-system.

For the insurance sector specifically, companies are increasingly looking at the issue not only as potential victims of cyberattacks but also as providers of solutions, notably by offering cyber insurance cover. The cyber insurance market in the EU is still at a nascent stage, especially compared to the US. However, the application of the legislation mentioned above, in particular the GDPR and NIS Directive, is expected to be a strong driver for the growth of the European cyber insurance market.

Finally, identification and global prosecution of the different cyber attack actors is becoming increasingly challenging in cyber space due to the lack of international jurisdiction agreements. Some efforts are already being undertaken, but more will have to be done to overcome challenges brought on by a global challenge such as cyber.

Next Steps

In conclusion, cybersecurity is not only about securing the weakest link in the chain: public and private institutions need to collaborate closer to find technical and legal tools to prevent and mitigate cyber attacks.

Financial Industry Committee

Aareal Bank
Accountancy Europe
Association for Financial Markets in Europe (AFME)
Banco Bilbao Vizcaya Argentaria (BBVA)
Banco Santander
Barclays
BlackRock
Bloomberg
Chartered Financial Analyst – Institute (CFA)
Commerzbank AG
Crédit Agricole
Danske Bank
Deloitte
Deutsche Bank AG
Euroclear
Eurofinas - Leaseurope
European Association of Public Banks (EAPB)
European Banking Federation (EBF)
European Fund and Asset Management Association (EFAMA)
European Money Markets Institute (EMMI)
European Payment Institutions Federation (EPIF)
European Savings and Retail Banking Group (ESBG)
Federation of European Securities Exchanges (FESE)
Goldman Sachs International
NEX Group
ING
International Swaps and Derivatives Association (ISDA)
Insurance Europe
Intesa Sanpaolo
JP Morgan
KBC
KPMG
Liechtenstein Bankers Association (LBA)
London Stock Exchange Group (LSEG)
Nasdaq
NVB – Dutch Banking Association
PensionsEurope
PricewaterhouseCoopers
S&P Global
Société Générale
State Street
Swiss Finance Council
TheCityUK
UBS AG
UniCredit Group
Union Asset Management Holding AG
VISA Europe
Western Union International
Zurich Insurance Company

Steering Committee

Nedzhmi Ali MEP
Burkhard Balz MEP (Chair)
Brando Benifei MEP
Kostas Chrysogonos MEP
Daniel Dalton MEP
Esther De Lange MEP
Pilar Del Castillo MEP
Mady Delvaux MEP
Herbert Dorfmann MEP
Frank Engel MEP
Ashley Fox MEP
Neena Gill MEP
Ana Maria Gomes MEP
Roberto Gualtieri MEP
Antanas Guoga MEP
Brian Hayes MEP
Roger Helmer MEP
Monika Hohlmeier MEP
Gunnar Hökmark MEP
Danuta Maria Hübner MEP
Catalin Sorin Ivan MEP
Eva Kaili MEP
Othmar Karas MEP
Sean Kelly MEP
Wolf Klinz MEP
Georgios Kyrtsos MEP
Alain Lamassoure MEP
Boguslaw Liberadzki MEP
Olle Ludvigsson MEP
Ivana Maletic MEP
Roberta Metsola MEP
Siegfried Muresan MEP
Sirpa Pietikäinen MEP
Georgi Pirinski MEP
Godelieve Quisthoudt-Rowohl MEP
Dominique Riquet MEP
Paul Rübig MEP
Andreas Schwab MEP
Davor Škrlec MEP
Ivan Stefanec MEP
Theodor Dumitru Stolojan MEP
Kay Swinburne MEP (Vice-Chair)
Michael Theurer MEP
Ramon Tremosa i Balcells MEP
Beatrix von Storch MEP
Steven Woolfe MEP
Auke Zijlstra MEP
Jana Zitnanska MEP

Briefing notes are prepared by the Financial Industry Committee to the European Parliamentary Financial Services Forum. For further information on the subjects raised in the briefs please contact the Chairman, Members or Secretariat of the Financial Industry Committee.

Chairman Financial Industry Members
Peter de Proft, Director General, EFAMA
Rue Montoyer 47, B-1000 Brussels
Tel: +32 2 513 39 69
E-mail: peter.deproft@efama.org

Secretariat
David Reed, EPFSF Director
2/4, Rond-Point Schuman, BE-1040 Brussels
Tel: +32 2 514 68 00
E-mail: secretariat@epfsf.org