EUROPEAN CENTRAL BANK

EUROSYSTEM

UNITAS Crisis communication exercise report

December 2018

Contents

Executive summary

On 28 June 2018 the Eurosystem's Market Infrastructure and Payments Committee (MIPC) carried out a market-wide crisis communication exercise. The exercise was conducted in the form of a facilitated discussion around a hypothetical scenario based on a cyber attack on major financial market infrastructures (FMIs), market infrastructures and service providers (collectively "financial infrastructures") resulting in a loss of data integrity.

The exercise was intended to: (i) raise awareness of data integrity issues and the implications for financial infrastructures; (ii) discuss how impacted financial infrastructures could cooperate and collaborate with each other and other relevant stakeholders on a pan-European basis; and (iii) assess the need for developing external public communication strategies.

Overall, the objectives of the exercise were met.

Participants acknowledged that the sharing of various forms of information, such as threat intelligence, incident data and even participant data, at the European level could be improved to enable swift recovery from an incident affecting the integrity of data.

More broadly, participants also noted that in the light of the increasing complexity of the financial ecosystem, there was a need for a better understanding of the operational interdependencies which could help improve European crisis management arrangements. A sector map could provide the basis for stakeholders to take a more structured approach to managing a major crisis triggered by cyber incidents – including both the operators of the financial infrastructures and their respective authorities.

Finally, participants emphasised the importance of staff training and awareness, to improve their abilities to respond to and recover from a major cyber incident.

1 Introduction

The European payments and settlement infrastructure has changed significantly over the last decade. The numerous domestic and cross-border systems that make up the European financial ecosystem are increasingly interdependent and interconnected through a web of direct and indirect relationships. Although these interdependencies take many forms, operational interconnectivity is at the heart of most financial infrastructures. Interdependencies have important implications for the safety and efficiency of the European financial ecosystem. Some forms of interdependencies have facilitated significant improvements in the safety and efficiency of payment and settlement processes, allowing the various parts of the ecosystem to interact with each other. But, equally, this has increased the potential impact of some risks on the ecosystem itself, most notably cyber risk. As the risk landscape continues to evolve rapidly, financial infrastructures will be exposed to potential cyber attacks, which could result in contagion across the system. To further complicate matters, the ecosystem is reliant on the safe exchange of data and if a financial infrastructure's data integrity is compromised in any way, it could have an adverse impact on the wider system. In the light of this, the MIPC conducted a tabletop crisis communication exercise based on a cyber scenario and tackling the specifics of a data integrity issue. The name "UNITAS" was chosen to reflect the core theme of the exercise, which was to promote collaboration and a united approach in managing cyber attacks affecting financial infrastructures in Europe.

This post-exercise report summarises the objectives of the exercise, the scenario, the key conclusions and the next steps.

2 Exercise objectives

The exercise aimed to:

- raise awareness of data integrity issues and their implications for financial infrastructures, as well as the importance of incorporating such scenarios into the respective entities' risk management frameworks;
- raise awareness of the specificities, differences and challenges of the individual financial infrastructures in dealing with a major data integrity issue;
- discuss how affected financial infrastructures could cooperate and collaborate with each other and with other relevant stakeholders on a pan-European basis;
- identify possible measures that could be taken by the interconnected financial infrastructures to enhance capabilities for effective data, information, incident and intelligence sharing among themselves and with other relevant stakeholders on a pan-European basis – including agreements, mechanisms and modalities;
- discuss the need for external public communication strategies for financial infrastructures on an individual, national and European level.

3 Organisation

The UNITAS exercise was a tabletop crisis communication exercise. All participants and observers convened at the ECB to conduct the exercise which engaged them in a facilitated discussion based on a pre-defined scenario concerning the threat and materialisation of a cyber attack on a financial infrastructure, and a number of pre-defined questions in two phases. In order to enable the participants to be actively involved in the discussion, they were grouped into different tables on the basis of the type of financial infrastructure they were representing. Each table had a moderator that guided the discussion around the pre-defined questions.

As the exercise was based on a facilitated discussion among the participants and not on a simulation, participants were not expected to react to the scenario in any operational capacity. Rather, the intention was to facilitate a dynamic discussion, allowing participants to provide their insights and experiences and identify common approaches taken in the prescribed scenario, as well as any gaps or shortcomings.

At the end of the two phases there was a collective discussion among all the participants, moderated by the exercise moderator. The final session of the day was a reflection on the exercise, guided by the exercise moderator, which focused on key lessons learned and how participants could work together collaboratively to address any identified issues and gaps and improve the resilience of the wider system.

It should be noted that participants were not evaluated and no oversight or supervisory judgement was made about their capabilities or the capabilities of the entity that they represented.

4 Exercise findings

4.1 Participants

Participants noted that, although it is not feasible to anticipate every possible scenario and scenarios change and evolve over time, it is important that each institution thoroughly considers all possible scenarios and indicators of compromise and embeds them in its incident management framework. Participants also emphasised that training, staff awareness and continuous testing are key, as is ensuring that a pro-active and risk-based culture is embedded within the financial infrastructure.

In terms of external engagement, participants noted that they would liaise with the national cybersecurity agencies, law enforcement agencies and overseers. At the European level, participants concluded that coordination between such agencies is needed, and there was an acknowledgement that this could be improved, which would certainly benefit the financial sector.

Participants also took note of the part of the scenario which indicated that other institutions were under attack and concluded that, while each institution would be prepared to respond to an attack by itself, the collective crisis management could be improved. Moreover, although each institution may have its own crisis management framework in place with its respective national authority being closely involved, coordination between institutions at the European level could also be improved.

On a broader point, participants noted that a European sector map, which could provide insight on the operational interdependencies of the financial infrastructures and their participants, would be useful. A sector map would identify the critical nodes within the ecosystem, how they are connected to other types of financial infrastructures and who are their corresponding authorities. Participants stated that such a map could provide the basis for improving existing European crisis management arrangements.

The participants also agreed that the recovery of a financial infrastructure in the case of compromised data integrity is complex. It entails several plausible scenarios pertaining to the creation, destruction, loss or alteration of data in transit or data at rest and, to recover the operations, the most critical activity would be to conduct a robust and comprehensive reconciliation between the affected actors and the financial infrastructure.

Overall, participants agreed that the financial ecosystem is largely comprised of various stakeholders (e.g. market infrastructures, banks and network service providers), all of whom have a shared responsibility to ensure that they undertake frequent reconciliation and consider possible alternative solutions for storing data. Therefore, participants agreed that the best option would be for all stakeholders to come together and explore common market practices, processes, tools, communication protocols and enforcement mechanisms to ensure that frequent

reconciliations are carried out effectively by the different types of financial infrastructures.

4.2 Overseers

From a market infrastructure oversight perspective, the overseers concluded in their discussion that they have a key role in communication, information sharing and coordination.

They agreed that there is a need to formalise arrangements for informing them of imminent threats (and of threat intelligence more broadly) and to have a harmonised approach to the reporting of such threats before they materialise in order to help other financial infrastructures prepare for possible attacks. They also stressed the importance of crisis communication and the secure channels that could be used by overseers, supervisors, other authorities and law enforcement agencies during such crises. To facilitate this, they noted that memoranda of understanding (MoUs) or other arrangements with relevant authorities and stakeholders would be necessary to facilitate secure communication channels, access to and sharing of information (e.g. on threats), and coordination across Europe.

All overseers have incident-reporting arrangements in place with their overseen market infrastructures to receive notifications of such major incidents in a timely manner. However, they agreed that there was room for improvement in how they notify other authorities or supervisors of financial infrastructures as well as supervisors of banks that participate in the financial infrastructures.

5 Key conclusions

Overall, the objectives of the exercise were met – the discussion raised awareness of data integrity issues and crisis communication following cyber attacks or other major operational disruptions. In particular, the participants:

- agreed on the complexity of the issues, acknowledging that each type of financial infrastructure faced different types of challenges and concluding that recovery from such a scenario required a new approach;
- concluded that such a recovery would require all stakeholders to come together and use a range of possible solutions to ensure that a coordinated reconciliation could take place in an efficient and timely manner;
- acknowledged that information sharing (including incident data and threat intelligence) at the European level could be enhanced and, more broadly, that crisis management arrangements could be improved, with clear structures, agreements and communication protocols based on a deeper understanding of the operational interdependencies.

6 Next steps

Based on the discussions during the UNITAS exercise, the following actions will be taken to strengthen the European financial system:

- Explore how to further enhance European crisis management arrangements. For example, based on a sector map of the European financial ecosystem, the crisis management arrangements could be operationalised by:

  (a) setting out the structures and protocols for cooperation between different stakeholders (including law enforcement and cybersecurity agencies) at a legal, operational and tactical level;

  (b) providing the legal framework for information sharing and establishing safe communication channels for all relevant stakeholders in moments of crisis;

  (c) outlining commonly agreed external communication strategies;

  (d) documenting a range of playbook scenarios, which are regularly tested at a collective level and facilitate increased training and awareness among all staff.

- Explore how best to conduct a coordinated recovery and reconciliation process, with common market practices, processes, tools and communication protocols. In addition, the financial infrastructures could explore technical solutions to improve how their data are protected and stored.

- Establish or update existing oversight MoUs or other arrangements with other authorities and relevant stakeholders to facilitate secure communication channels, access to and sharing of information, and coordination across Europe to manage major crisis scenarios, as well as establishing arrangements for the reporting and sharing of threats (and threat intelligence more broadly).

- Explore best practices around training and awareness.

As the above actions would have implications for the wider ecosystem, the Eurosystem and the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB)[1], established in 2018 by the ECB, will cooperate with the financial market infrastructures (FMIs), market infrastructures and service providers to implement these next steps.

[1] Information about the Euro Cyber Resilience Board can be found on the ECB's website.

7 Annex – UNITAS exercise attendees

Participants: Payment systems

- TARGET2
- EURO1
- STEP2-T
- CORE(FR)
- EMZ
- SNCE
- equensWorldline
- BI-Comp

Participants: Central securities depositories (CSDs) and central counterparties (CCPs)

- Euroclear
- Clearstream Banking AG (CBF)
- Monte Titoli
- Eurex Clearing
- LCH SA

Participants: Service providers and market infrastructures

- SWIFT
- SIA-Colt
- T2S

Participants: Central bank overseers

- European Central Bank
- Banque de France

- Nationale Bank van België/Banque Nationale de Belgique
- Deutsche Bundesbank
- De Nederlandsche Bank
- Banca d'Italia
- Banco de España

Observers

- European Securities and Markets Authority (ESMA)
- European Union Agency for Network and Information Security (ENISA)
- Eurosystem Internal Auditors Committee representatives
- MIPC members

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.ecb.europa.eu

For specific terminology please refer to the ECB glossary.

PDF ISBN 987-92-899-3679-8, doi:10.2866/519326, QB-03-18-552-EN-N