SPECIAL FEATURE A: CYBER-RELATED PAYMENT DISRUPTIONS: ASSESSING BANKS' LIQUIDITY RESILIENCE THROUGH T2[1]

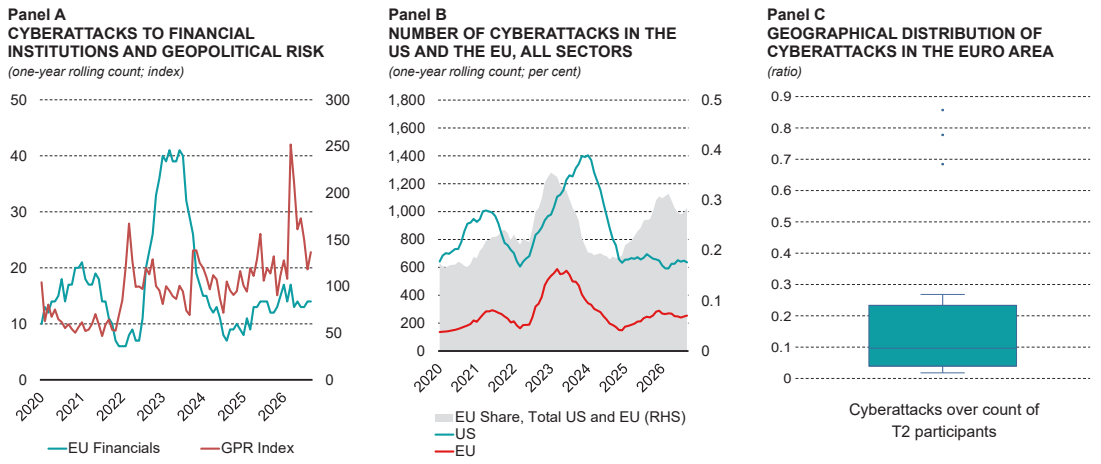
An evolving financial landscape

The rapid digitalisation of financial services has increased banks' dependence on interconnected payment infrastructures, core banking systems and third-party technology providers, making cyber risk increasingly relevant from a financial stability perspective. A severe cyber incident can extend beyond the immediate operational disruption and generate broader financial consequences.

Understanding and quantifying how liquidity stress propagates through payment and settlement systems is essential for assessing how a cyber incident can evolve from an operational disruption into a broader financial stability risk. Disruptions to critical banking services or uncertainty about the scope of an attack may undermine confidence in the affected institution, potentially triggering deposit outflows and increasing funding pressures. Meeting unexpected liquidity needs may require the sale of assets, potentially at a discount, thereby generating losses that could adversely affect a bank's solvency position and, in extreme circumstances, its viability (or going concern). As payment and settlement systems are highly interconnected, liquidity shortages can also spread to other institutions through delayed or missed payments, amplifying stress across the banking sector.[2]

Given the evolving financial landscape, cyber risks have attracted increasing regulatory and supervisory attention. As shown in Chart A.1, cyberattacks targeting the EU financial and insurance corporations have rebounded since 2024 lows but remain below their 2023 peak, while the number of cyberattacks per institution varies markedly across EU countries. The available data also indicates that reported cyberattack exposure is unevenly distributed across EU countries. This heterogeneity is particularly relevant when

Chart A.1
PUBLICLY DISCLOSED CYBER EVENTS AND GEOPOLITICAL RISK



Sources: University of Maryland Cyber Event Database; ECB; Authors' calculations.

Notes: Panel A illustrates the 12-month rolling count of publicly disclosed cyberattacks to financial and insurance corporations and the GPR Index by Caldara, D., & Iacoviello, M. (2022); Panel B depicts the 12-month rolling count of all the publicly disclosed cyberattacks to US and EU across all sectors, and showing the share of EU cyberattacks on the right-hand axis; Panel C presents the distribution across euro area countries of the number of cyberattacks targeting financial and insurance corporations from 2020 per credit institution that is a direct participant in the national T2 component system (calculated using observations following the migration from TARGET2 to T2 in 2023).

[1] Written by Matteo Panfilo and Francesco Ricciutelli, Senior Research Economists, and Kanan Musayev, Senior Economist within the Stress Testing and Research Office of the Central Bank of Malta. The authors would like to thank Mr Alan Cassar, Ms Christine Balzan, Mr Pedro Polvora for their helpful comments as well as Mr Edward Magro, Ms Tiziana Grech, Mr Shaun Vella, Mr Paul Azzopardi and Ms Abela Ritlen, for technical assistance on T2.

[2] A special feature published in FSR 2025 applies transaction-level data from T2 to map the topology of payment flows and identify key interlinkages, critical nodes and connections within Malta's payment system.

assessing exposures to foreign financial institutions that are significant net senders of payments. In this context, the ECB's 2024 cyber resilience stress test assessed banks' ability to respond to and recover from a severe cyber incident. In parallel, the Digital Operational Resilience Act has strengthened the EU framework for ICT risk management, incident management and reporting, and resilience testing.

Against this background, this study assesses the Maltese banking system's resilience to a cyber-induced liquidity disruption, focusing on how the shock may be transmitted through the payment network. By applying the Bank of Finland Payment and Settlement System Simulator (BoF-PSS3), and based on Eisenbach (2020), this exercise simulates a liquidity-sink scenario in which a selected institution is unable to execute outgoing payments while continuing to receive incoming funds. The resulting interruption to liquidity flows may affect counterparties that normally rely on the disrupted flows to fund their own obligations, creating potential second-round effects across the network. The tool allows payment and liquidity outcomes under the stressed scenario to be compared to a baseline simulation that represents normal payment activity.

The analysis quantifies the effects of liquidity being temporarily removed from circulation by identifying the banks most exposed to the resulting suspension or delay of incoming payments, and by assessing the potential direct and second-round effects on payment settlement and liquidity positions. The exercise employs T2-Malta transactions for the fourth quarter of 2025. It simulates one-day and three-day liquidity-sink scenarios involving the largest domestic direct participants and the largest foreign senders of payments to Maltese banks. The resulting liquidity deterioration is subsequently translated into changes in banks' Liquidity Coverage Ratios (LCRs) to assess the extent to which regulatory liquidity buffers may come under pressure. In doing so, the exercise moves beyond the operational impact on the initially affected institution and provides a quantitative assessment of how a cyber-related payment disruption could translate into broader financial stability effects.

The Bank of Finland Payment and Settlement System Simulator: its application to a liquidity disruption

BoF-PSS3 is an analytical simulation tool developed by the Bank of Finland to study liquidity needs and risks in payment and settlement systems. The simulator is widely used by central banks and the research community for payment-system analyses, scenario analyses and stress testing.[3,4]

The tool supports a wide range of payment and securities settlement structures, including real-time gross settlement (RTGS), deferred net settlement, continuous net settlement, hybrid, retail and large-value payment systems, as well as securities settlement systems. At a minimum, BoF-PSS3 requires transaction data only, but simulations can also incorporate account balances, intraday credit limits, bilateral and multilateral limits, system events and reservations. The resulting outputs support the analysis of liquidity consumption, settlement volumes, queuing and gridlock, counterparty risk and the role of critical participants.

An important feature of BoF-PSS3 is its application to scenario analyses and stress testing. Financial distress scenarios are generated by modifying the underlying input data or system configuration.[5] The framework can represent a range of disruptions, including participant defaults, cyber-attacks, and other operational incidents, by allowing stressed outcomes to be compared with the normal functioning of a system. The study focuses on a one-day cyber event and, subsequently, calculates average daily impacts in Q4 2025. It also considers a three-day disruption, as described below. PSS3 establishes a

[3] Its application in recent research further illustrates its relevance for stress-testing exercises. Khiaonarong et al. (2025) use BoF-PSS3 as a cyber stress-testing framework, applying it to transaction-level TARGET Services data to simulate cyber disruptions and assess their impact on payment settlement and liquidity risk. Similarly, Laine and Korpinen (2021) employ the PSS3 to analyse the resilience of the Finnish payment system to liquidity-sink shocks and resulting contagion effects.

[4] Bank of Finland Payment and Settlement System Simulator.

[5] Depending on the shock applied, a scenario can involve cancelling, delaying or reordering transactions, changing beginning-of-day balances or credit limits, modifying bilateral or multilateral limits, or altering system setups, algorithms and account structures.

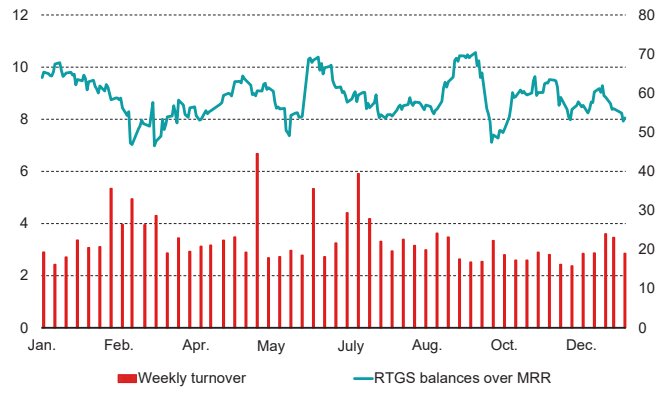
baseline of payment activity calibrated using T2 transactions and subsequently imposes a liquidity-sink scenario. This simulates an interruption of ICT services, preventing T2 Direct Participants (both foreign and domestic participants, determined on the basis of T2-Malta activity and their relevance to domestic banks) from forwarding orders through the RTGS to other domestic participants. Following Eisenbach et. al (2020), the shock is introduced by preventing the affected bank from executing outgoing payments. The liquidity impact is estimated by comparing the stressed simulation with the baseline scenario. This comparison enables the calculation of counterfactual end-of-day balances and the quantification of unsettled transactions.

An environment characterised by a strong level of reserves

Malta's current ample-reserves environment reflects a prolonged process of liquidity accumulation, originating in the aftermath of the Global Financial Crisis and subsequently reinforced by the ECB's implementation of non-standard monetary policy measures.

In 2009, the introduction of fixed-rate full-allotment refinancing operations, together with significant disruptions in interbank markets, generated substantial excess liquidity within the Maltese banking system. Banks obtained approximately €1.2 billion through LTROs.[6] This liquidity-rich position, coupled with high levels of wholesale and retail deposits, remains a structural feature of the banking system. By 2018, core domestic banks reported an aggregate LCR exceeding 184%, while non-core and international banks reported an average LCR of 415.5%, with liquid assets largely comprising central bank reserves and sovereign securities.[7] The expansionary monetary policy measures adopted during the COVID-19 pandemic further strengthened this position: between early 2021 and February 2022, excess liquidity in the Maltese banking system increased from approximately €5.5 billion to €6.6 billion,[8] predominantly in the form of excess reserves held with the central bank. Throughout 2025, available RTGS balances remained broadly equivalent to around eight to ten times regulatory reserve requirements, while average weekly payment turnover accounted for only about 20% of available balances (see Chart A.2). Overall, the structurally abundant level of excess liquidity – relative both to regulatory requirements and to ordinary payment and settlement needs – provides an important buffer against liquidity disruptions. The analysis, therefore, focuses on the structure of transaction flows, systemically relevant institutions and the geographical concentration of payment senders.

Chart A.2
RTGS BALANCES AND TURNOVER IN 2025
(ratio; per cent (RHS))



Sources: T2; Authors' calculations.
Notes: RTGS Balance divided MRR (LHS); weekly turnover is calculated by averaging the absolute value of inflow and outflows, to then divide by the amount available for RTGS transactions (RHS).

Simulating the liquidity impact of cyber disruptions in T2-Malta

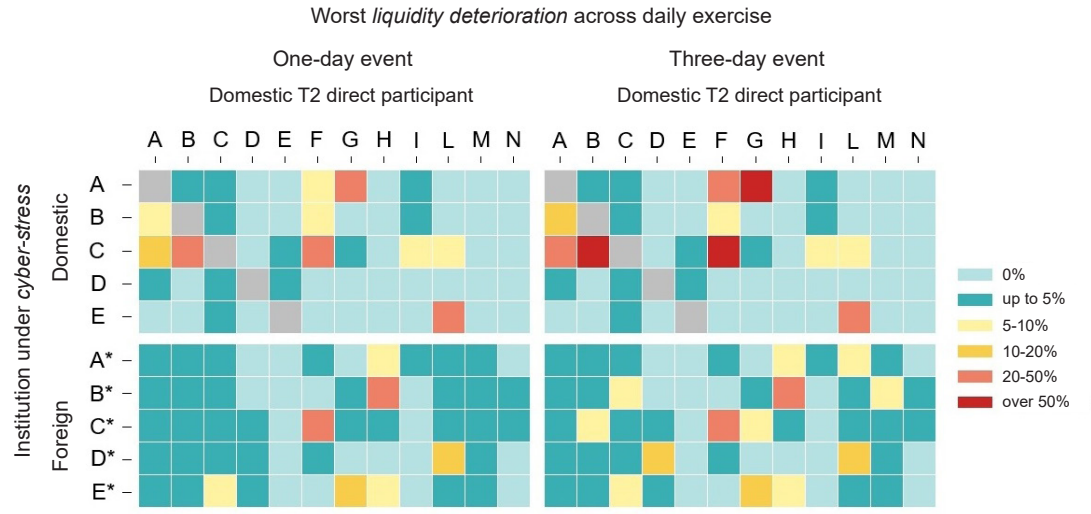
A simulation exercise was conducted using BoF-PSS3 and T2-Malta payment system data to quantify the liquidity implications of a hypothetical cyber event. This exercise stresses the top five most active T2 domestic direct participants[9] and the top five foreign

[6] Central Bank of Malta (2009), *Annual Report* 2009.
[7] Central Bank of Malta (2018), *Interim Financial Stability Report* 2018.
[8] Central Bank of Malta (2022), Central Bank of Malta *Quarterly Review* 2022.
[9] Those involved in higher exchanged value for the quarter.

senders (from Germany, Austria and France)[10] to domestic direct participants, by imposing an independent liquidity-sink behaviour. For each liquidity-sink of interest (i.e., the bank under cyber pressure), the exercise runs a separate simulation for each operational day in the fourth quarter of 2025, assuming the target bank cannot send payments for the entire day,[11] but continues to receive funds from other T2 participants. In this framework, each liquidity sink represents a single scenario, composed of a set of independent simulations involving each day in the quarter. This approach allows the estimation of scenario-specific statistics by averaging the indicators across days, or by picking the worst-case liquidity deterioration for the stressed quarter. The exercise is then repeated by prolonging the simulation to a three-day event starting on each day of 2025Q4 to study more severe scenarios through a rolling window.[12]

Figure A.1 shows the simulated cyber-stress scenarios for one-day, and prolonged to three-days, by distinguishing between T2-Malta direct participants and foreign banks. Each row identifies the liquidity-sink of five domestic and five foreign banks, while the columns represent the 12 Maltese T2 Direct Participants. Cell colours indicate the magnitude of the liquidity deterioration, showing how the simulated reductions vary with both the origination and duration of the cyber event. The results indicate that some domestic banks appear closely linked to specific network participants, with multi-day disruptions causing liquidity deterioration to accumulate to potentially severe levels. A number of institutions could be affected simultaneously. This highlights the degree of dependency among domestic banks and the most active T2-Malta direct participants. When foreign participants drive cyber-incidents, liquidity shocks tend to affect a broader set of domestic banks, although the resulting magnitude of impacts generally remains more contained.

Figure A.1
LIQUIDITY DETERIORATION MATRIX, DAILY EXERCISES FOR Q4 2025

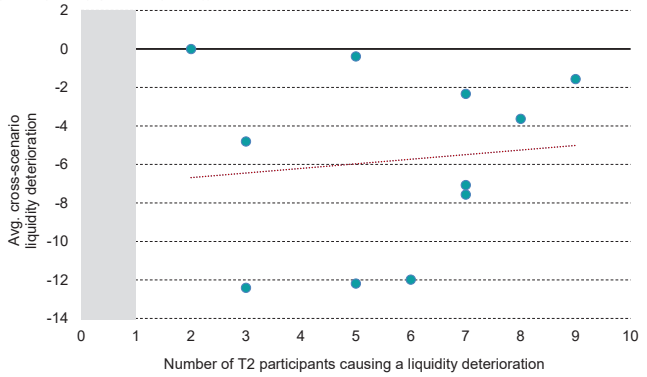


Sources: T2; Authors' calculations.
Notes: Cells represent the maximum liquidity deterioration of T2-Malta Direct Participants (x-axis) which other T2 participants (y-axis) might potentially cause if unable to send payments on any day of Q4 2025. Liquidity deterioration is measured as the percentage end-of-day deviation from baseline RTGS balances due to the missing inflow related to the cyber-event.

[10] For more information on geographical breakdown and domestic network, please see "Special Feature: Using T2 to assess payment-system flows relevant for cyber stress testing in Malta" (*Financial Stability Report* 2025).
[11] For the purposes of this study, direct debits and analogous payments directed to ancillary systems are excluded from the sample of payment orders processed by the simulator, thereby restricting the analysis to payer-initiated payment instructions.
[12] In this framework, the impacts originated by a three-day event are the result of cumulating one-day impacts and assumes that the affected bank still continues to provide liquidity even though it is not receiving any from the liquidity sink. This can underestimate the quantification of second-round effects whereby banks would react to the liquidity sink behaviour to preserve their liquidity stance and this impact is not being captured.

Chart A.3 shows, for any bank, the number of T2 participants that may cause a positive deterioration in its liquidity position when acting as a liquidity sink,[13] and the bank's average worst-case liquidity deterioration across those liquidity sinks.[14] The first measure, shown on the x-axis, captures the number of potential sources from which cyber-induced liquidity stress can propagate through the payment network. The second measure, shown on the y-axis, captures the average severity of their impact, calculated by averaging the largest liquidity decline caused by each impactful liquidity-sink across the simulated days. Together, these measures allow banks to be compared in terms of both the breadth and severity of their simulated payment-network exposure.

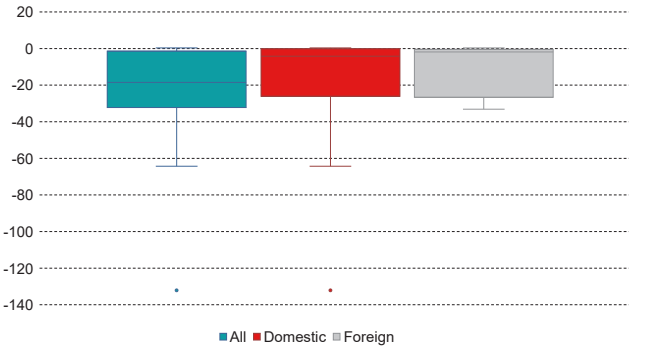
Chart A.3
COUNT OF CONNECTIONS CAUSING LIQUIDITY PRESSURE VERSUS AVERAGE WORST-CASE LIQUIDITY DETERIORATION
(count (x-axis); per cent (y-axis))



Sources: T2; Authors' calculations.
Notes: Each point represents a bank; the y-axis shows the average of maximum liquidity deterioration (across liquidity sinks); the x-axis the number of T2 participants that cause such liquidity erosion (i.e. the count of x-axis average components); quadrants are identified by median values.

The two measures are weakly positively correlated, although individual banks show different patterns of simulated exposure. Some banks record substantial liquidity deterioration in the simulations despite being exposed to relatively few problematic connections. By contrast, another small group is exposed to more participants causing liquidity deterioration but records smaller average maximum liquidity declines, although these remain above the sample median. These differences indicate that exposure to more sources of stress within the simulated network does not necessarily coincide with more severe liquidity deterioration.

Chart A.4
DISTRIBUTION OF WORST-LCR SHIFTS
(per cent)



Sources: T2; Authors' calculations.
Notes: counterfactual LCR shifts are calculated by differencing actual LCR and the one obtained after adjusting the LCR using the worst-case liquidity deterioration produced by the simulations; for any impacted bank, the amount of Q4 2025 HQLA is adjusted by subtracting the cross-scenario maximum liquidity deterioration (i.e. the worst liquidity deterioration observed across days and liquidity sinks). Such an adjustment term is firstly picked from the pool of domestic scenarios; secondly, from the pool of scenarios that involves foreign banks and then includes all domestic and foreign.

Impact on liquidity coverage

The analysis investigates further the potential for severe liquidity deterioration in terms of the regulatory threshold of 100% for the LCR.[15] Chart A.4 shows that cyber-stress scenarios generally deteriorate banks' LCR, with negative shifts across all scenario groups.

[13] Given the business model of certain Maltese banks, as well as their transactional structure as T2 participants, a subsample of banks cannot be impaired when the liquidity-sink is applied to specific domestic or foreign banks.

[14] The y-axis reports the average worst-case liquidity deterioration across scenarios, where each scenario corresponds to a T2 participant acting as a liquidity sink and involves multiple daily simulations over Q4 2025. For each scenario, the maximum daily liquidity deterioration is first identified. These worst-case values are then averaged across scenarios to obtain the value reported on the y-axis.

[15] Defined as per *Commission Delegated Regulation (EU) 2015/61*. The RTGS balance is part of Level 1 HQLA, therefore the reduction is assumed to affect the numerator of the LCR, while net liquidity outflows over the 30-day stress horizon are kept unchanged. The resulting decline in the LCR, measured in percentage points, equals the balance shortfall expressed as a percentage of net liquidity outflows. The scenarios are deliberately mechanical, whereby affected banks do not seek alternative liquidity in the money market or through Eurosystem facilities, counterparties do not stop paying the sink, and no contingency arrangements are activated. The results therefore measure liquidity at risk before any mitigating or amplifying response, rather than forecasts of actual outcomes.

Scenarios involving domestic participants show a more pronounced tail of larger LCR reductions, while those involving foreign participants are more concentrated around relatively modest LCR reductions.

With an average LCR of 478% in Q4 2025, the banks included in the exercise entered the simulated scenarios with substantial liquidity buffers. Although the worst-case shocks cause a significant liquidity deterioration, LCRs remain well above the 100% regulatory minimum. The results therefore suggest that these ample reserves provide a strong buffer against cyber-induced liquidity stress. Disruptions originating at some domestic participants generate sizeable liquidity reduction, while those originating from foreign participants affect a broader set of domestic banks but generally have a more limited impact. Nevertheless, some banks record substantial simulated liquidity deterioration following disruptions to a small number of counterparties on particular days. These findings illustrate how payment-network analysis can complement traditional liquidity indicators by identifying concentrated payment-flow dependencies that may leave individual banks vulnerable despite ample overall liquidity buffers.

Concluding remarks

This article assesses how a cyber incident that prevents a domestic or foreign bank from sending payments through T2, could affect the liquidity position of other banks operating in Malta. Using the BoF-PSS3 and T2-Malta transaction data for the fourth quarter of 2025, it simulates one-day and three-day liquidity-sink scenarios for the five largest domestic direct participants and the five largest foreign senders of payments to Maltese banks. The resulting liquidity reductions are expressed as percentage changes in affected banks' liquidity balances as well as in terms of changes to their LCR.

The results suggest that the ample reserves held by Maltese banks help to absorb cyber-induced liquidity stress transmitted through T2 under the simulated scenarios. Within this framework, the results highlight the importance of payment-flow concentration alongside the aggregate level of liquidity. A small number of domestic T2 participants act as critical sources of incoming payments for specific banks, and a liquidity sink at one of them can generate sizeable liquidity reductions, particularly if the disruption lasts several days or coincides with days of unusually large flows. Larger simulated reductions arise when a disruption at a relevant participant coincides with days of high transactional concentration, so the timing of an incident matters as much as the institution it hits. Foreign participants transmit disruptions more widely across the system, but with smaller effects on individual banks.

These findings suggest that monitoring of payment-network dependencies, including the concentration of each bank's incoming payments by counterparty and by country of origin, could complement traditional liquidity indicators, which capture the size of buffers but not their exposure to the failure of specific participants. Banks' liquidity contingency plans and digital operational resilience testing could benefit from scenarios in which a key counterparty stops paying for several days, alongside the disruption of the bank's own systems; arrangements that allow an affected participant to continue settling its most critical payments would also limit the liquidity withdrawn from the system (Kosse and Lu, 2022).

Going forward, the framework could be extended to help define a systemic cyber tolerance threshold, based on the severity and duration of participant-specific disruptions and their potential system-wide effects. This analysis could also inform escalation criteria within contingency and crisis management frameworks. The scenario design could also move beyond single-participant disruptions to include simultaneous disruptions in groups of smaller banks, disruptions propagated through common third-party providers, and more widespread or prolonged interruptions to cross-border payment inflows. Test scenarios can also comprise simulations of malicious insider knowledge of single entities or system wide peak vulnerability patterns to maximise a harmful impact. Furthermore, the analysis could be expanded to incorporate banks' reserves and portfolio management responses to assess how adverse liquidity scenarios could impact their solvency positions. In particular, this extension could examine whether heightened liquidity pressures trigger forced asset liquidations and whether the resulting losses materially weaken banks' capital positions.

References

Bedford, P., Millard, S. and Yang, J. (2004), "Assessing Operational Risk in CHAPS Sterling: A Simulation Approach", Bank of England *Financial Stability Review*, June, pp. 135–143.

Bedford, P., Millard, S. and Yang, J. (2005), "Analysing the Impact of Operational Incidents in Large-Value Payment Systems: A Simulation Approach", in Leinonen, H. (ed.), Liquidity, Risks and Speed in Payment and Settlement Systems – A Simulation Approach, Bank of Finland *Scientific Monographs* No. E:31.

Clarke, A. and Hancock, J. (2012), "Payment System Design and Participant Operational Disruptions", *Research Discussion Paper* RDP 2012-05, Reserve Bank of Australia.

ECB (2017), "Stress-Testing of Liquidity Risk in TARGET2", *Occasional Paper Series* No. 183, European Central Bank.

Eisenbach, T.M., Kovner, A. and Lee, M.J. (2022), "Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis", *Journal of Financial Economics*, 145(3), pp. 802–826.

Heijmans, R. and Wendt, F. (2020), "Measuring the Impact of a Failing Participant in Payment Systems", IMF *Working Paper* WP/20/81, International Monetary Fund.

Khiaonarong, T., Korpinen, K.N. and Islam, E. (2025), "Using Simulations for Cyber Stress Testing Exercises", IMF *Working Paper* WP/2025/085, International Monetary Fund.

Kosse, A. and Lu, Z. (2022), "Transmission of Cyber Risk Through the Canadian Wholesale Payment System", Bank of Canada Staff *Working Paper* 2022–23.

Kotidis, A. and Schreft, S.L. (2025), "The Propagation of Cyberattacks through the Financial System: Evidence from an Actual Event", *Journal of Finance*, 80(6), pp. 3313–3358.

Laine, T. and Korpinen, K. (2021), "Measuring Counterparty Risk in FMIs", *BoF Economics Review*, No. 9/2021, Bank of Finland, Helsinki.

Ledrut, E. (2007), "How Can Banks Control Their Exposure to a Failing Participant?", in Leinonen, H. (ed.), Simulation Studies of Liquidity Needs, Risks and Efficiency in Payment Networks, Bank of Finland *Scientific Monographs* No. E:39, Chapter 8.

Leinonen, H. and Soramäki, K. (2003), "Simulating Interbank Payment and Securities Settlement Mechanisms with the BoF-PSS2 Simulator", Bank of Finland *Discussion Paper* 23/2003.