INTERNATIONAL MONETARY FUND

Using Simulations for Cyber Stress Testing Exercises

Tanai Khiaonarong, Kasperi Korpinen, Emran Islam

WP/25/85

2025
MAY

WORKING PAPER

 WP/25/85

IMF Working Paper
Monetary and Capital Markets Department

Using Simulations for Cyber Stress Testing Exercises

Prepared by Tanai Khiaonarong, Kasperi Korpinen, and Emran Islam*

Authorized for distribution by Jay Surti
May 2025

ABSTRACT: We demonstrate how computer-based simulations could support cyber stress testing exercises through a three-step framework. First, cyber-attack scenarios are designed to target the systemic nodes of a payment network at different times, disrupting a major bank, critical service provider, large-value payment system, and a foreign exchange settlement system. Second, the stress resulting from the scenarios is simulated using transaction-level data, and its impact is measured through a range of risk metrics. And third, cyber preparedness is discussed to identify effective practices that could strengthen the cyber resilience of the financial sector. The exercise provides insights into the main vulnerabilities of the financial sector and key transmission channels under plausible scenarios that necessitate preemptive action and recovery and response measures. For example, simulation results for Finnish data suggest that end-of-day liquidity risk is most severe when a cyber-attack hits a major bank or several banks simultaneously through dependence on a common critical service provider, compared to an attack on a centralized payment system where effective queuing and liquidity-saving mechanisms can better support recovery. Outcomes could be aggravated under more severe and prolonged scenarios.

RECOMMENDED CITATION: Khiaonarong, T., K. Korpinen., and E. Islam. (2025). Using Simulations for Cyber Stress Testing Exercises. Working Papers WP/25/85, International Monetary Fund.

JEL Classification Numbers:	C63, E42, E58, G17, K24, L86
Keywords:	Cyber Resilience; Stress Testing; Simulation
Author's E-Mail Address:	tkhiaonarong@imf.org; kasperi.korpinen@bof.fi; eislam@imf.org

* The authors would like to thank Jay Surti and Dirk Jan Grolleman for their comments and input. Kasperi Korpinen served as an IMF Visiting Scholar during the research and the support from the Bank of Finland is gratefully acknowledged. Marie-Bernadette Amand de Mendieta provided editorial assistance. One of the authors of this paper is a member of one of the user groups with access to TARGET data in accordance with Article 3 of the Decision (EU) 2023/549 of the European Central Bank (ECB) of 6 March 2023 on access to and use of certain TARGET data and repealing Decision ECB/2010/9 (ECB/2023/3). The Bank of Finland and the Market Infrastructure Board (MIB) of the ECB have checked the paper against the rules for guaranteeing the confidentiality of transaction-level data imposed by the MIB pursuant to Article 5 of the above-mentioned issue. The views expressed in the paper are solely those of the author(s) and do not necessarily represent the views of the Eurosystem.

WORKING PAPERS

Using Simulations for Cyber Stress Testing Exercises

Tanai Khiaonarong, Kasperi Korpinen, Emran Islam

Contents

1. Introduction

Cybersecurity risk is a growing concern for macro-financial stability, but how bad could it get?[1] We investigate this question in this paper. Many jurisdictions have made continuous efforts to strengthen their cyber resilience, through the development of cybersecurity strategies and regulations for their financial sectors; strengthening the supervision and oversight of cybersecurity risks and of adherence to regulations; establishing Computer Emergency Response Teams (CERT), ensuring adequate information sharing, incident reporting; and introducing testing and crisis simulation exercises. Such efforts continue to face challenges associated with an evolving threat landscape that reflects the interaction of growing digital technologies and supply chains with geopolitical tensions and criminal activities.

Cyber-attacks have already disrupted critical functions in the financial system, including payment, clearing, settlement, and custodial services and impacted systemically important financial entities, such as systemically important banks, interbank payment systems, central securities depositories, and stock exchanges.[2] Such entities serve a critical role in financial markets and have distinct risk profiles (CPMI-IOSCO, 2012). In many cases, financial sector authorities and the industry have coordinated closely with respect to crisis communications to safeguard financial stability and maintain public confidence. In some jurisdictions, authorities have made proactive efforts to counter such threats, including running cyber stress tests to test the responses and cyber preparedness of retail payments and the database of banks' operating systems.[3]

For the purpose of this paper, the term cyber stress testing is used interchangeably with scenario-based testing. This is distinct from penetration testing and red team testing methods which are commonly used to assess cyber resilience; and other stress testing methods used to assess credit, liquidity, and operational risks (Cihak, 2007). This interpretation adheres to the Committee on Payments and Market Infrastructures and the Technical Committee of the International Organization of Securities Commissions (CPMI-IOSCO) Guidance on Cyber Resilience for Financial Market Infrastructures (FMIs), hereafter referred to as "Cyber Guidance".

On scenario-based testing, the Cyber Guidance states: *"Tests should address an appropriately broad scope of scenarios, including simulation of extreme but plausible cyber-attacks, and should be designed to challenge the assumptions of response, resumption, and recovery practices, including governance arrangements and communication plans. FMIs should use cyber threat intelligence and cyber threat modelling to the extent possible to imitate the unique characteristics of cyber threats. They should also conduct exercises to test the ability of their staff and processes to respond to unfamiliar scenarios, with a view to achieving stronger operational resilience."*[4]

[1] According to a cross-country study, the financial sector has a large share of cyber events as compared to other industries (Harry and Gallagher, 2018). For a discussion on the financial stability implications of cybersecurity risks, see Adelman et al., (2020) and IMF (2024).

[2] For example, cyber-attacks in the banking sector have targeted interbank payment systems with prolonged outages (Ukraine, January 2024; Lesotho December 2023); a subsidiary of a global systemically important bank was subject to a cyber-attack that interrupted some of its operating systems used to clear trades in government securities and caused payment delays (United States, November 2023); and in the securities sector, cyber-attacks were experienced by central securities depositories (India, November 2022) and stock exchanges (New Zealand, August 2020).

[3] See the cyber stress testing exercises of the Bank of England, Danish Financial Supervisory Authority, and European Central Bank.

[4] See MITRE ATT&CK for information on adversary tactics and techniques based on real-world observations that could be used to develop specific cyber threat models. For the development of incident handling scenarios and sample questions, see Cichonski et al., (2012).

This paper proposes a cyber stress testing framework for financial sector authorities such as central banks by applying computer-based simulation methods to assess the impact of cyber incidents on financial stability. The objective is three-fold: (i) to assess the quantitative impact on settlement and liquidity according to a range of risk metrics; (ii) to strengthen cyber incident response and recovery, ecosystem resilience, and situational awareness with policy considerations; and (iii) to complement tabletop cyber exercise programs with quantitative assessments to support decision-making. The framework and simulation tool provides authorities with a practical approach to assess the financial stability implications of cyber security risks.

The methodology is guided by and builds on earlier simulation analyses and stress testing studies of operational risks in payment networks, which was pioneered at the Bank of Finland and used widely by national central banks and the research community (Annex 1).[5] This methodology uses computer-based simulations—a payment and settlement systems simulator—which is a key component of the framework used to simulate stress in the cyber exercises.[6] The simulator is a software application that enables the replication of the key features of a payment system, including computer algorithms that simulate the movement of actual payment transactions data across participants and systems (Annex 2).

Simulations replicate actual systems and data to help make a quantitative assessment. For example, this could involve participant default, cyber-attacks, terrorist attacks, operational incidents, bank runs, collateral devaluation, supply chain attacks, and system or policy changes. Direct and systemic effects could be measured, including settlement delays, settlement failures, queues, account liquidity positions at end-of-day, liquidity usage, and liquidity deterioration. The use of computer-based simulations to assess the impact of cyber risks remains at an early stage, and in our view, has potential to complement existing testing arrangements.[7]

While the case of Finland is used for illustrative purposes in this paper, the lessons are highly relevant for emerging market and developing economies. First, authorities such as central banks, banking authorities, and securities regulators, have supervisory and oversight responsibilities for systemically important financial institutions and infrastructures—the critical and systemic nodes in a financial system. Second, some authorities—mainly central banks—also have major operational responsibilities such as operating the large-value payment system (LVPS), retail payment systems such as check clearing systems and fast payment systems, central securities depository, or securities settlement system of a country. And third, many authorities have a statutory mandate to safeguard financial stability, which could include analyzing the impact of a cyber-attack on the financial system and preparing an effective response, recovery, and resumption plan. Key

[5] See Leinonen, 2005, 2009; Hellqvist and Laine, 2012; Laine, 2015; Heijmans and Wendt, 2020. For earlier simulation studies, see Humphrey, 1986; McAndrews and Wasilyew, 1995. Following the major, wide-ranging disruptions related to the events of September 11, 2001, the topic of operational risks and their financial stability implications gained closer attention from financial authorities and systems operators (McAndrews and Potter, 2002; Lacker, 2003). Economic studies of cyber-attacks on the financial system and their impact on financial stability is also emerging in the academic literature. See Eisenbach et al., 2020; Kotidis and Schreft, 2022.

[6] The Bank of Finland's payment and settlement systems simulator has been made publicly available to the central banking and academic community for research purposes and is subject to licensing from the Bank of Finland. Apart from the Bank of Finland, payment simulators have also been developed by other national central banks, academia, and private firms for proprietary use.

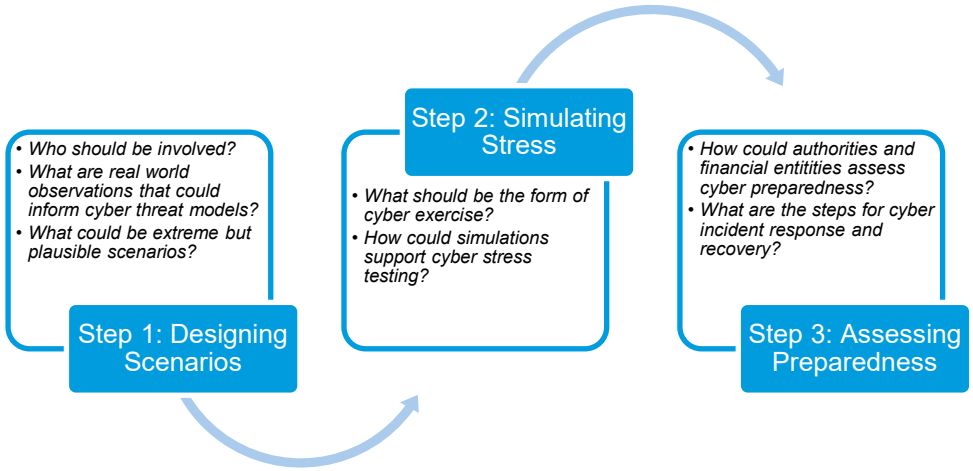
[7] For example, Kosse and Lu (2022) used the simulation approach to study the transmission of cyber risk in a LVPS and explored three scenarios, including: a cyber-attack on one bank; an attack on multiple banks; and a situation where there is partial impairment of payment capacity. The authors conclude that the system-wide impact of a cyber-attack could be significantly reduced through contingency arrangements that enable banks that are subject to cyber-attacks to still submit high-value payments. They also highlight the importance of cyber resilience at both system and participant levels and the need for strong sectoral collaboration and coordination. See also, G-7 Fundamental Elements of Cyber Exercise Programs.

lessons from the simulation exercises reported in this paper include the following. First, timely systems recovery and effective queuing and liquidity risk management could generally serve as preemptive actions to reinforce cyber resilience. Second, financial sector entities that have a mature CIRR framework will be best placed to respond and recover from the incident, therefore reducing the risk to the system. Third, as with other types of financial sector stress tests, an adequately wide range of stress scenarios can be expected to be of significant use to the industry in strengthening risk management and to authorities in their surveillance of safety, soundness and financial stability.

2. Simulating Stress in Cyber Exercises: A Framework

The framework for cyber stress testing is organized into three main steps, including: (i) designing scenarios, (ii) simulating stress, and (iii) assessing preparedness (Figure 1). Each step is discussed as follows.

Figure 1. Framework for Simulating Stress in Cyber Exercises



Source: Authors.

Step One—Designing Scenarios

The first step of the cyber stress testing framework involves the design of scenarios. Five plausible scenarios are presented below where four involve a cyber-attack on a systemic node in the financial system. The scenarios are informed by past operational and cyber incidents.[8] For all scenarios, the impact involves operational disruptions to payment systems above two-hours—the international standard for the recovery time objective (RTO) of critical information technology systems that underpin systemically important FMIs. Assumptions are used for the purpose of the simulations and to inform the discussions on the response, recovery, and resumption of services after a cyber incident. The scenarios may not reflect other relevant factors

[8] Khiaonarong et al., (2021) study recent operational outages in electronic payment systems which helped guide the planning of plausible scenarios in this paper.

such as bank behavior that could differ during normal and stressed conditions. Cyber incidents may also be unresolved within the same business day or spill over to the next day or weekend leading to inter-day exposures. News or rumors can rapidly (e.g., through social media), or eventually, escalate an incident into a crisis. Market structure could also influence concentration risk.

Scenario 1. Ecosystem operates in normal conditions without incidents (baseline).

Overview: The LVPS operates under normal conditions without any cyber-attacks. Banks have access to an unaltered amount of liquidity provided by the central bank. This establishes the benchmark simulation scenario.

Scenario 2. Systemically important financial institution is targeted by cyber criminals.

Overview: A major bank (Bank) is the target of an external denial of service attack. The affected bank is the largest participant in terms of market share of transaction values in the LVPS and stops the submission of outgoing payments for four hours in the afternoon. Initial investigation results confirm the cybersecurity incident. The FMI regulator and relevant authorities are notified. Other banks stop outgoing payments to the affected bank two hours before the closing time. Notification of cybersecurity incident is delayed to end-of-day. Contingency measures lack manual paper-based procedures for processing time-critical transactions in extreme circumstances.

Assumptions: Security controls of the affected bank are compromised and exploited. Such controls include weaknesses in security updates, password policy, multi-factor authentication, malware protection, physical security, vulnerability scanning, or other controls.[9] Defense-in-depth approach is deficient, including the layered protection of physical, logical, and administrative access controls. Anomalies in network traffic, unusual activity in user account, and high authentication failures indicate compromise. Training on cyber hygiene is deficient. The settlement cycles of ancillary systems (such as a retail payment system) that are linked to the LVPS operate normally after anomalies.

Scenario 3. Critical service provider (CSP) to financial sector is hit and experiences an outage.

Overview: A CSP is the target of an attack exploiting an application server. The affected CSP provides data processing and information systems management services to the five largest banks, including its core-banking activities. The CSP data breach affects the confidentiality and integrity of payment instructions. The five largest banks are unable to submit payment instructions for four hours in the afternoon before the closing time. Notification of cybersecurity incident is delayed to end-of-day. Contingency measures lack manual paper-based procedures for processing time-critical transactions in extreme circumstances.

Assumptions: The attack assumes that malicious actors gain access to data contained in a server-side application (database) or on the server of the CSP. Ransomware was used to steal access credentials and manipulate data. The CSP is critical as it generates environmental interdependencies, as the five largest banks have a common reliance on the company as a third-party information technology provider with cloud services. The scenario is aggravated with the lack of regular audits of the CSP. The settlement cycles of ancillary systems that are linked to the LVPS operate normally after anomalies.

Scenario 4. Central bank compromised by an insider threat.

Overview: A central bank owned and operated LVPS is the target of an internal denial of service attack. The affected system experiences an outage for 10-hours, including at the primary and secondary sites. All banks

[9] To help mitigate cybersecurity risks, industry efforts have been made to require financial firms to self-attest and audit security controls. For illustration, the SWIFT 2023 Customer Security Control Framework consists of 32 security controls (24 mandatory controls and 8 advisory controls). Standard-setting bodies have also catalyzed the operationalization of a global strategy to reduce the risk of wholesale payments fraud related to endpoint security (CPMI, 2018).

are unable to submit payment instructions 10-hours after opening time. Notification of cybersecurity incident is delayed to end-of-day. Contingency measures include manual paper-based procedures for processing high priority and time-critical transactions in extreme circumstances between opening and closing time. The affected system resumes after closing time and operational hours are extended until midnight to continue settlements.

Assumptions: An insider threat affects access and data losses and disrupts operations.[10] The system's security policy was deficient in terminating system access of a former employee who worked as a system administrator and has knowledge of the technical architecture and weaknesses of the organization. Based on the exit interview, the former employee demonstrated grudges against the organization and resigned on less-than-favorable terms. The attack occurs in a highly regulated and secured system, which is has been designated a systemically important payment system that observes international standards. The settlement cycles of ancillary systems that are linked to the LVPS operate normally after anomalies.

Scenario 5. Systemically important financial infrastructure faces an advanced persistent threat.

Overview: A privately-operated foreign exchange (FX) settlement system is the target of an attack exploiting an application server. The affected system provides cross-border and multi-currency payment services. The data breach affects the confidentiality and integrity of payment instructions. The outage occurs for five hours (7:00 am to 12:00 pm Central European Time) and affects interbank payments in the LVPS. All banks are unable to submit or receive payment instructions during the window for settlement and funding of the system. Notification of cybersecurity incident is delayed to end-of-day. Contingency measures lack manual paper-based procedures for processing time-critical transactions in extreme circumstances.

Assumption: The attack assumes that malicious actors gain access to data contained in a server-side application (database) or on the server of the company. Ransomware was used to steal access credentials and manipulate data. The FX settlement system is critical as it generates environmental interdependencies, as all banks have a common reliance on the system to settle foreign exchange transactions. The system also plays an important role in reducing foreign exchange settlement risks in the global foreign exchange market. The settlement cycles of ancillary systems that are linked to the LVPS operate normally after anomalies.

Table 1 summarizes the cyber stress scenarios and assumptions used in this paper.

Table 1. Cyber Stress Scenarios

Scenario	Assumptions	Risk Metrics 1/
1. Baseline	▪ Payment system operates under normal conditions. ▪ Banks have access to unaltered amount of liquidity.	▪ Total value of unsettled payments ▪ Total volume of unsettled payments ▪ Average queue value ▪ Delay indicator
2. Bank	▪ External denial of service attack affects payment controls. ▪ Bank system outage of 4-hours. ▪ Bank is unable to submit outgoing payments 4-hours in the afternoon before closing time. ▪ All banks stop outgoing payments to affected bank 2-hours before closing time. ▪ Bank is the largest participant in terms of market share of transaction values.	

[10] See CISA (2020) for a description of insider threats and mitigation strategies.

		▪ Notification of cybersecurity incident is delayed to end-of-day. ▪ Contingency measures lack manual paper-based procedures for processing time-critical transactions in extreme circumstances. ▪ The settlement cycles of ancillary systems that are linked to the large-value payment operate normally after anomalies.	▪ Maximum liquidity deterioration ▪ Minimum liquidity deterioration
3.	CSP	▪ Attack exploits application server and affects confidentiality and integrity of payments. ▪ CSP outage of 4-hours. ▪ 5 largest banks are unable to submit payment instructions 4-hours in the afternoon before closing time. ▪ CSP provides ICT services to the 5 largest banks in terms of market share of transaction values. ▪ Notification of cybersecurity incident is delayed to end-of-day. ▪ Contingency measures lack manual paper-based procedures for processing time-critical transactions in extreme circumstances. ▪ The settlement cycles of ancillary systems that are linked to the large-value payment operate normally after anomalies.	
4.	LVPS	▪ Internal denial of service attack through insider threat affects access and data. ▪ LVPS outage of 10-hours, including at the primary and secondary sites. ▪ All banks are unable to submit payment instructions 10-hours after opening time. ▪ Contingency measures include manual paper-based procedures for processing high priority and time-critical transactions in extreme circumstances between opening and closing time. ▪ Notification of cybersecurity incident is delayed to end-of-day. ▪ LVPS resumes after closing time and operational hours extended until midnight to continue settlements. ▪ The settlement cycles of ancillary systems that are linked to the large-value payment operate normally after anomalies.	
5.	FX	▪ Attack exploits application server and affects confidentiality and integrity of payments. ▪ FX settlement system outage of 5-hours (7:00 a.m. to12:00 p.m. Central European Time). ▪ All banks are unable to submit to or receive payment instructions from the FX system during the window for settlement and funding. ▪ Contingency measures lack manual paper-based procedures for processing time-critical transactions in extreme circumstances. ▪ Notification of cybersecurity incident is delayed to end-of-day. ▪ FX settlement system resumes after outage. ▪ The settlement cycles of ancillary systems that are linked to the large-value payment operate normally after anomalies.	

Source: Authors.

Note: 1/ Risk metrics are defined in the Bank of Finland's Payment and Settlement Simulator User Manual. See also Table 3 of this paper.

Step Two—Simulating Stress

The second step of the cyber stress testing framework is the simulation of cyber stress. This involves the collection of actual payment systems data, replicating the features of an actual payment system in a computer-based simulator, and running the simulations with the data for each cyber stress scenario. Stress is created by introducing anomalies into the datasets (Table 2).

Data

For simulation purposes we used TARGET Services data for February 2024. The data includes all payments and transfers, account balances, credit line changes, bilateral limits and reservations related to the Central Liquidity Management (CLM) and Real-Time Gross Settlement (RTGS) components. The reported results include only metrics related to the participants of TARGET Services that are accessing through the Bank of Finland. For a typical business day, there could be over 400,000 transactions. That is, one month can amount to more than 8.4 million transactions. In February 2024, there were 8.76 million transactions. This puts challenges on the computing resources needed in terms of memory, processing power, and software design.

Methodology

To perform the analysis, we use simulations that replicate the settlement logics of the TARGET Services components: CLM and RTGS. The RTGS is basically the same as the former TARGET2 but without central bank liquidity management operations related to central bank facilities that were moved to CLM. The segregation of operations to different technical components makes the account structure more complex and induces a need for cross-component liquidity transfers.

Simulations were run with the Bank of Finland's Payment and Settlement System Simulator (BOF-PSS). Tailored algorithms made for the Eurosystem were used to replicate TARGET Services. More precisely, the automated stress testing tool of the simulator was used, allowing the dynamic generation of scenarios without recreating copies of the original input data.[11]

The simulations performed in this study are the first ones run for the TARGET Services and their design involved a number of important considerations associated with the automated stress tester, reporting functionalities and database indexes. The choices made under these individual dimensions in terms of optimization and streamlining of processes were highly consequential. For example, they led to improvements in the performance of running Scenario 1 (Baseline) with the stress tester (including the upper bound run) from around six hours to under two hours. The time needed to run a one-month benchmark simulation was improved from around three and a half hours to one hour.

Each scenario involved the development of new tailored query filters. The automated stress tester allows the user to define the participants and accounts to be affected. For each scenario, the challenge was to identify the types of transfers and payments to be affected (Table 2). The types of transfers affected and anomaly time

[11] This process helps saves gigabytes of storage space. This is done by using SQL-filters that define the modifications to be done to the input data defining the scenario of each simulation. The stress tester also uses parallelization of simulations which speeds up significantly the running of the simulations in function of the available cores.

intervals are defined in the scenario specific query filters. Six risk metrics are used to compare changes in performance and risks for the different scenarios (Table 3).[12]

Table 2. Data Adjustments for Scenarios

Scenario	Data Adjustments
1. Baseline	Not applicable.
2. Bank	All payments introduced by Bank after 2:00 p.m. and all payments sent towards Bank introduced after 4:00 pm are removed. Automated payments remain in the simulations.
3. CSP	Outgoing payments of the five biggest banks introduced after 2:00 p.m. are removed from the simulations. Incoming payments remain in the simulations.
4. LVPS	All introduction times of payments and transfers between 2:30 a.m. and 12:30 p.m. are postponed until 12:30 p.m. Earliest debit times during that period are also postponed until 12:30 p.m. Latest debit times occurring between 2:30 a.m. and 12:30 p.m. are postponed until 1:30 p.m. to give more time for settlement.
5. FX	All introduction times of payments and transfers between 7:00 a.m. and 12:00 p.m., involving the FX settlement system, are postponed until 12:00 p.m. Earliest debit times during that period are postponed until 12:30 p.m. to allow the possibility for single transfers to be executed before batches. Latest debit times occurring between 7:00 a.m. and 12:00 p.m. are postponed until 1 p.m. to give 30 minutes time for settlement.

Source: Authors.

Table 3. Description of Risk Metrics

Risk Metric	Description
Total value of unsettled payments	The sum of the values of the unsettled transactions in a simulation or scenario. These would correspond to the sum of unsettled payments due to the direct scenario effect, or in other terms the payments removed from the simulations, and the payments unsettled in the simulations also referred to as systemic or second-round effects due to the altered situation in the scenarios.
Total volume of unsettled payments	The count of the unsettled transactions in the simulation or scenario. These would correspond to the systemic or second-round effects due to the altered situation in the scenarios.
Average queue value	The average time weighted value of queue balance.
Delay indicator	The delay indicator is a relative indicator ranging from 0 to 1. If no transactions are queued the value is 0 if all transactions are queued the maximum time, namely from entry time till the end of the day, the value is 1. The value is calculated as the time weighted queue value for each transaction. In other terms the sum of the products of transaction values multiplied by the times in queue is divided by the sum of the products transaction values multiplied by the maximum theoretical time the payment could have delayed in queue. A mathematical formulation is provided in the simulator's manual.
Maximum liquidity deterioration [1/]	The needed extra liquidity to keep end of day (EOD) balance in the scenario, unchanged when other participants are not able to compensate and cannot send all of their payments. Maximum Liquidity Deterioration = End of day

[12] For further details on the risk metrics, see the Bank of Finland's Payment and Settlement Simulator User Manual. Intraday throughput is an additional risk metric that could be used but is not within the scope of this study.

	balance in benchmark simulation - End of day balance in scenario + unsettled in scenario (systemic) - Unsettled in benchmark (systemic). It reflects the needed extra liquidity to settle all unsettled payments and achieve same level of end of day liquidity as in the benchmark. It is assumed that other participants are not able to bring in extra liquidity intraday. If the value is negative, it is an improvement and it is rounded to 0.
Minimum liquidity deterioration	The needed extra liquidity to keep end of day (EOD) balance in the scenario, unchanged when other participants are able to compensate and still send their unsettled payments. Minimum Liquidity Deterioration = End of day balance in benchmark simulation - End of day balance in scenario + unsettled in scenario (systemic) - Unsettled in benchmark - incoming unsettled (systemic, not direct) in scenario. It reflects the needed extra liquidity to settle all unsettled payments and achieve same level of liquidity as in the benchmark. It is assumed that unsettled incoming payments are settled and the buffers of other participants are sufficient, and they are able to bring in extra liquidity. If the value is negative, it is an improvement and it is rounded to 0.

Source: Authors.

Notes: 1/ The maximum and minimum liquidity deteriorations were first used in Laine and Korpinen (2021). The main idea of these indicators is to quantify the liquidity risks involved in scenarios at participant level. More precisely, the metric measures how much extra liquidity the participants would need to be able to bring to the system in order to keep their end of day account balance unchanged compared to the benchmark. The maximum and minimum liquidity deteriorations define a plausible interval inside which the real liquidity impact could fall.

Results and key observations

Confidentiality aspects related to the underlying data limit the level of details we can disclose results for publication purposes. Internally, within the source entity of the data, these limitations do not apply the same way allowing for deeper analysis. For example, it is possible to bring the analysis to participant level which indeed brings very interesting insights to mutual counterparty exposures between participants.[13]

The simulation results for each scenario are summarized in Table 4. The unsettled payments here include the originally unsettled payments due to the scenarios and the subsequent unsettled payments in the outcome of the simulations also referred to as second-round effects. The originally unsettled payments due to the scenarios are the payments not made to the counterparts of the entities experiencing the event. These are also referred to as the direct effect. In practice, Scenarios 2 (Bank) and 3 (CSP) are created by dropping payments out of the simulations (see Table 2). The volume of unsettled payments is simply the respective count of the same unsettled payments included in the values. For more details on the calculation of the underlying indicators please refer also to Table 3.

To obtain the unsettled values and volume, the unsettled transactions were first summed up to daily level, after which a simple average was taken over the days. The account level indicators were first aggregated to the level of days and then averaged to obtain a single figure. The queue value is a daily time-weighted average of the sum of transactions in queue averaged over the days. The delay indicator is calculated on a daily level as explained in Table 3 and then averaged over the days. The liquidity deteriorations are sums on a daily level which have been averaged to one figure as well.

[13] See Korpinen and Laine (2021) who present a methodology to assess counterparty risks of participants in TARGET2.

Table 4. Simulation Results from Cyber Stress Testing

Scenario	Value of unsettled payments (€ million)	Volume of unsettled payments (number of transactions)	Queue value (€ million)	Delay indicator	Liquidity deterioration (Min) (€ million)	Liquidity deterioration (Max) (€ million)
1. Baseline	0.20	0.05	0.49	0.0039	0.00	0.00
2. Bank	190.61	51.70	0.48	0.0039	1.80	23.12
3. CSP	2,676.54	295.95	0.47	0.0048	0.00	23.09
4. LVPS	0.20	0.05	0.48	0.0039	0.00	0.00
5. FX	0.42	0.10	0.68	0.0039	0.20	0.20

Source: Authors.
Note: Figures are simple averages over the simulation days and rounded. For the volume of unsettled payments, the averaged figures reflect a few unsettled transactions in Scenarios 1, 4 and 5.

Regarding the unsettled payment indicators, it should be noted that in the reported figures, there are practically no second-round effects, and almost all effects are direct effects related to the scenarios. The baseline value of 0.2 comes from one observation on one day which is present in all scenarios. Only Scenario 5 (FX) has a second-round contagion effect, but only on one day and it amounts to around 4 million euros explaining the slightly higher average value of 0.42 instead of 0.2. This also explains the small value difference in the queue value. It is also sufficiently small to not affect the delay indicator. This second-round effect is also observable as a small change of 0.2 in the liquidity deterioration indicators. Would this not have been the case, it would have been interesting to report the direct effects and secondary effects separately. It is also noteworthy that as the input data contains real payments the inherent network information is also included in the results. The difference in unsettled payments between Scenarios 2 (Bank) and 3 (CSP) is directly attributable to the direct effects of the scenarios. The start and end times of the events are practically the same and in Scenario 3 (CSP), there are more removed payments.

Two key observations with respect to financial stability implications could be drawn. The first observation is that the most severe impact on settlement and liquidity risks occurs with a hit on a major bank or multiple banks through a critical service provider. The simulation results demonstrate these impacts in terms of unsettled payments and liquidity deteriorations under Scenarios 2 (Bank) and 3 (CSP). This is due to the initial severity or direct effect of the scenarios characterized by the definitive removal of the payments affected by the scenarios, whereas in Scenarios 4 (LVPS) and 5 (FX), payments are only delayed leaving a possibility for settlements to resume. The results show that this is indeed the case, and the level of unsettled payments remains close or same to the benchmark with the exception of one day for Scenario 5 (FX) as described.

Figure 2 shows the distributions of the daily aggregated values of the total sums of liquidity deteriorations. Scenarios 4 (LVPS) and 5 (FX) do not materialize liquidity risks except for the one-day exceptional observation for Scenario 5 (FX). This is also why Scenarios 4 (LVPS) and 5 (FX) were left out from Figure 3. The box plot shows that the variance over the days is larger for Scenario 2 (Bank) than for Scenario 3 (CSP). The liquidity deteriorations are slightly larger but also more consistent between days. This is also probably because more participants were directly affected by the event. When daily observations are examined, liquidity deteriorations were not experienced on many days or multiple accounts (Figure 3). Only a small number of accounts have

liquidity deteriorations on different days whereas a majority of accounts did not have liquidity deteriorations on most of the days.

Combining the information of not having second-round effects while observing end of day liquidity deteriorations we can deduct that liquidity available on the accounts were sufficient to absorb the liquidity risk while being able to settle other due payments.

Figure 2. Sum of Maximum Liquidity Deteriorations Over Participants Per Simulation Day

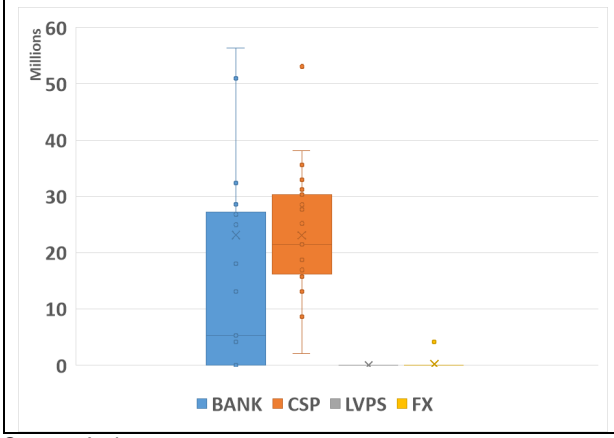
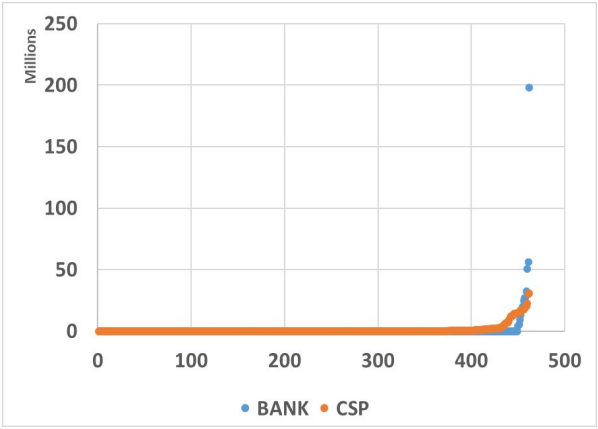


Figure 3. Liquidity Deteriorations Per Account and Day



Source: Authors.

Note: In Figure 2, the Y-axes represent the sums of liquidity deteriorations per day. Cases where accounts face liquidity increases are counted as 0, equal to no liquidity deterioration. In Figure 2, the dots are sums of daily observed liquidity deteriorations. For presentational reasons, Figure 2 was scaled so that one high value daily observation is not visible. In Figure 3, the Y-axes represent the amount of liquidity deterioration per account, whereas each dot represents an account on a specific day. The X-axis is simply the count of observations.

A hit on a systemically important financial institution or third-party service provider could impact financial stability through three transmission channels—loss of confidence, lack of substitutability, and interconnectedness. Under Scenarios 2 (Bank) and 3 (CSP), the 4-hour outage could lead to a loss of confidence. Lengthier and recurring outages could eventually lead customers and market participants to lose confidence in the financial system. Attacks and outages affecting one firm may lead to the perception that other firms are similarly vulnerable. Liquidity is also likely to be affected quickly if confidence is lost. And if the third-party also provides a monopolistic service, the lack of substitutability also poses a risk.

The second main observation is that the impact on settlement and liquidity risks from a hit on centralized payment systems was mitigated with queuing and liquidity-saving mechanisms. The simulation results suggest that recovery was close to 100 percent in terms of unsettled payments and queue indicators for Scenarios 4 (LVPS) and 5 (FX).

The queue and delay indicators indicate that the recovery is fast. In Scenarios 4 (LVPS) and 5 (FX), due to the scenarios, the payments are delayed to a later time in the day. The payment delays due to the direct effect of the scenarios are not reflected in the delay and queue indicators as the scenarios are built by introducing the payments later to the settlement process in the simulations. This means the initially delayed payments are not put to the payment queue in the simulation for the event's time and are introduced for settlement at the end of

the event. This still leaves potential for possible subsequent delays or queueing after the end of the event. The fact that the values of the queue and delay indicators stay low indicates that the payments affected by the event are settled extremely fast after the end of the event and that contagion effects are also indistinguishable with these metrics. In other terms, the scenario delays, and changes in the settlement order of payments do not create deadlocks nor lead to unsettled payments. This also means that, as the simulator follows the algorithmic routines of the production system without manual intervention, the results shows that at least there is a theoretic possibility of near complete and fast recovery from the anomalies of both scenarios.

This could be largely explained by the hybrid nature of TARGET's RTGS module which has queueing and liquidity saving mechanisms. Because payments are queued and queue releasing offsetting algorithms are run relatively frequently, it is possible to observe this positive result in the simulations. It is important to note here that we assumed in the simulations, that ancillary system cycles can be postponed freely until the end of the anomalies and there is no obstacle to run them after without delays. The simulator makes this possible as the ancillary system batches and payments remain in queues or are postponed to the end of the anomaly.

The queue release mechanisms of TARGET allow the liquidity provision transfers related to ancillary system settlements to take place and the subsequent batch processes and queue releases to occur. This is an important outcome, as this indicates that if automation is at a high level, manual procedures are minimized. TARGET Services are also allowed to resume without external restraints with the given transaction set and could well resume from the anomaly very efficiently.

It can also be noted that Scenarios 2 (Bank) and 3 (CSP) did not put significant pressure on the liquidity saving mechanisms as the direct effect was the removal of payments close to the end of the day and the indicators did not show any second-round effects like payments piling up in the queues and additional unsettled payments. Further insight could be obtained by comparing the processes that settled the payments and whether there was a shift from entry settlement towards reliance on liquidity saving mechanisms. The low levels and quasi-immutability of the delay indicator and queue values make this unlikely.

For Scenarios 2 (Bank) and 3 (CSP), the absolute number of affected payments also remains low. For Scenario 2 (Bank), the average number of unsettled payments is 52 per day and Scenario 3 (CSP) is 296. These figures seem a priori manageable even in case of switching to partially manual operations. For Scenarios 4 (LVPS) and 5 (FX), the number of payments affected is not deductible from Table 4 as the payments were mainly delayed.

Assumptions and issues

Before proceeding to the final step of the cyber stress testing framework in the next section, we revisit some of the assumptions and lessons learned. The exercise reinforces the importance of resuming business operations in a timely manner, having effective measures to manage liquidity risk, and minimizing unsettled payments. This resonates with the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI) and Cyber Guidance, where the latter notes the following.[14]

"Financial stability may depend on the ability of an FMI to settle obligations when they are due, at a minimum by the end of the value date. An FMI should design and test its systems and processes to enable the safe

[14] We focus on selected points from the PFMI and Cyber Guidance for the purpose of this paper. A comprehensive analysis against all the relevant principles of the PFMI or components of the Cyber Guidance is beyond the scope of this study.

resumption of critical operations within two hours of a disruption and to enable itself to complete settlement by the end of the day of the disruption, even in the case of extreme but plausible scenarios. Notwithstanding this capability to resume critical operations within two hours, when dealing with a disruption FMIs should exercise judgment in effecting resumption so that risks to itself or its ecosystem do not thereby escalate, whilst taking into account that completion of settlement by the end of day is crucial. FMIs should also plan for scenarios in which the resumption objective is not achieved. Although authorities recognize the challenges that FMIs face in achieving cyber resilience objectives, it is also recognized that current and emerging practices and technologies may serve as viable options to attain those objectives. Furthermore, the rationale for establishing this resumption objective stands irrespective of the challenge to achieve it."

The simulation results, however, could have been aggravated with more severe and prolonged scenarios. In fact, cybersecurity incidents could involve longer outages than 4 to 10 hours as assumed in this study. Such incidents could extend to multiple days or weeks, complicating system restoration, resumption, and end-of-day settlement. For authorities responsible for the cybersecurity supervision and oversight of the financial sector, the simulation results therefore suggest the importance of involving and coordinating work with authorities tasked with financial stability analysis, banking supervision, FMI operations and oversight, financial market operations, and resolution.

The simulations raise practical questions with respect to operational risk management. For FMI operators and banking supervisors, these include the following. What conditions would necessitate the extension of the operational hours of a payment system, and if so, for how long? What alternative arrangements are in place (for example, manual paper-based procedures) to allow for the processing of time-critical transactions in extreme circumstances? How many staff would be needed to manually process such transactions? What should be done if the settlement cycles of ancillary systems that are linked to the payment system fail to operate normally after a cyber-attack? When should a temporary suspension from the payment system be invoked for a bank that experienced a cyber-attack? What if end-of-day settlement could not be achieved and unsettled payments remain until the next business day or week? Should a central bank consider queuing and liquidity-saving mechanisms as part of the modernization of its RTGS system?

The exercise also highlights how liquidity and foreign exchange settlement risks could arise for unsettled payments. For all the scenarios, it is assumed that access to central bank intraday liquidity facilities is available, and this helps manage potential liquidity risks. What if payment transactions were based on a "pure" RTGS, which operates with prefunding arrangements and without access to central bank intraday liquidity facilities? What if there are liquidity shortages due to collateral deterioration (ECB, 2017)? Which bank could face intraday liquidity risks after a cyber-attack (BCBS, 2013a)? What are the foreign exchange settlement risk that could arise from inter-day exposures due to the differences in time zones and settlement hours of counterparties and systems, respectively (BCBS, 2013b)? Does the value of an unsettled foreign exchange transaction exceed the available liquid capital of a given bank (Korpinen and Laine, 2021)?

Such questions are illustrative and non-exhaustive and could help inform the design of more extreme but plausible scenarios.

Step Three—Assessing Preparedness

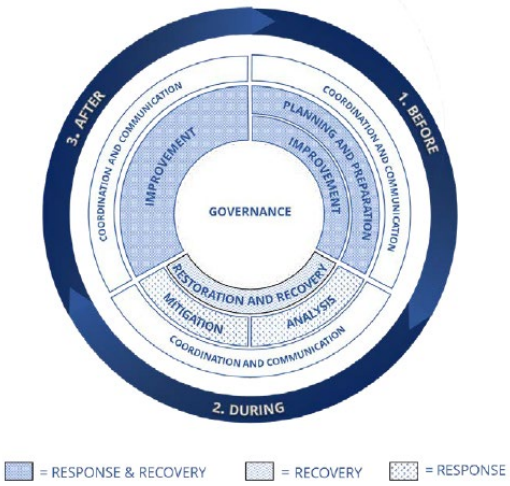
The third step of the cyber stress testing framework involves assessing cyber preparedness. The scenarios stressed in this paper have highlighted the potential systemic impact of a cyber incident and accentuate the importance of crisis preparedness and response and recovery for financial sector entities. This section sets out key principles and approaches that financial entities, regulators and supervisors should consider, to strengthen their response and recovery arrangements at a micro and macro level.

Steps for financial entities—Cyber Incident Response and Recovery Framework

Financial entities should ensure that they have a comprehensive Cyber Incident Response and Recovery (CIRR) framework in place. A CIRR framework will enable an entity to execute the appropriate activities in reaction to a detected or reported cyber incident, as well as carry out the appropriate activities to restore any systems, capabilities or resume services or operations that were impaired due to a cyber incident. An effective and comprehensive CIRR framework should combine a number of components, ensuring a financial entity is prepared to respond and recover before, during and after an incident (Box 1).

Box 1. Cyber Incident Response and Recovery Framework

Governance: The CIRR framework should be predicated on effective governance arrangements. An effective governance structure should define the decision-making framework with clear allocation of responsibilities and accountabilities to ensure that the right internal and external stakeholders are engaged when a cyber incident occurs. It is useful to identify an individual or a team to coordinate actions and communications for a cyber incident, with clear reporting and escalation paths to management, in the event of an incident.



Planning and preparation: The CIRR framework should adequately set out planning and preparation activities, so that the entity is prepared to respond before an incident occurs. Entities should establish policies, ex-ante, to prepare and plan for responding and recovering from a cyber incident. Policies should include relevant high-level statements that drive the development of more detailed plans and playbooks. For instance, policies should, among other things, address the classification and the assessment of cyber incidents and include a clear communication strategy and plan, which describe whom to inform of the cyber incident within a given timeframe. Entities should establish and maintain plans and playbooks that provide well-defined, organized approaches for CIRR activities, including criteria for activating the measures to expedite the organization's response time. Entities should develop an adequate number of plans and playbooks for specific purposes (e.g. response, recovery, contingency, communication) that align with the overall cyber resilience strategy. Such plans and playbooks should cover the initial hours and days of a cyber incident, which are usually the most critical. Furthermore, entities should establish their communication

strategies for internal and external stakeholders. This entails developing a communications plan and pre-defined statements to address different types of cyber incidents. Finally, entities' plans and playbooks should include severe but plausible cyber scenarios and stress tests that are based on high-impact, low-probability events and scenarios. These may include ransomware, Distributed Denial of Service (DDoS), system intrusion, data exfiltration, and system disruption. These scenarios and stress tests should be regularly assessed in business continuity tests and CIRR exercises. Annex 3 provides an example of questions that could be used to lead discussions during tabletop or crisis simulation exercises.

Analysis: During an incident, entities should have the capabilities to conduct analysis, including forensic analysis, and determine the severity, impact, and root cause of cyber incidents to drive appropriate and effective CIRR activities. Having the capacity to conduct such analysis and investigation during an incident improves an entity's capacity to determine the impact of a cyber incident and respond accordingly.

Mitigation: Entities should be prepared to activate mitigation measures to prevent the aggravation of the situation and eradicate cyber incidents in a timely manner to alleviate their impact on business operations and services. Mitigation can take four forms: 1) containment, where entities activate their containment measures and technologies best suited to each type of cyber incident to prevent the incident from inflicting further damage, including to connected entities; 2) business continuity measures, where entities invoke business continuity plans to maintain critical operations based on a pre-defined prioritization process; 3) isolation, where entities decide whether to shut down or isolate all or substantial parts of their systems and networks, as opposed to maintaining their business services operations; and 4) eradication, where entities remove all materials and artefacts (i.e. malicious code and data) introduced by the attacker. The specific type of mitigation measure depends on the nature of the cyber incident and requires timely judgement during an incident.

Restoration and recovery: The CIRR Framework should direct entities on how to restore and recover their systems and services. It is essential that entities give due consideration on how to recover and restore systems and services in a safe and timely manner, ensuring that no risk is brought to the system as a whole. Entities should prioritize recovery activities based on the criticality of business operations, systems and supported services that drive security and restoration requirements. In order to classify the criticality of processes and systems, metrics like RTO and Recovery Point Objective (RPO) or tiered criticality levels should be used and decided in advance of an incident. It is essential that entities validate that restored assets are free of compromise, fully functional and meet the security requirements before returning the systems to normal business operations for resumption of services.

Coordination and communication: Across the life cycle of a cyber incident, entities need to coordinate with their trusted stakeholders to ensure the effective management of the incident and protect the wider ecosystem in which they operate. During a cyber incident, entities must escalate cyber incidents to relevant stakeholders within the organization (and outside) to avoid delays in addressing the incident. Timely

escalation to the entities' decision-makers is essential for the acceleration of CIRR actions, which include seeking approval and authorization to implement response and recovery plans. Entities should also inform relevant stakeholders about potential business disruptions caused by the cyber incident, the response and recovery activities taken and the plans to restore services. The frequency and intervals of such updates should be set in advance to manage expectations, and this accentuates the importance of playbooks and testing ex-ante.

Improvement: Incidents are inevitable, and there will always be important lessons to learn from them, to further improve the CIRR Framework. Consequently, entities should establish processes to improve CIRR activities and capabilities through lessons learnt from both proactive tools, such as CIRR exercises, tests and drills, and past cyber incidents.

Source: Financial Stability Board (2020).

Financial entities should have an agile and evolving CIRR framework in place, that encompasses all the components cited above. Each aspect of the CIRR framework interconnects with each other and allows an entity to be prepared for an incident in a holistic manner.

The scenarios set out in this paper demonstrate that a cyber incident has the potential to become systemic and pose a threat to the wider system, and in such cases, entities that have a mature CIRR framework will be best placed to respond and recover from the incident, therefore reducing the risk to the system. In Scenarios 2 (Bank) and 3 (CSP), the CIRR framework would be particularly relevant. Within this context, it is therefore essential that prudential authorities work closely with their supervised entities to ensure that they have an effective, comprehensive and mature CIRR framework in place.

While the impact was softened with effective queuing and liquidity-saving mechanisms in Scenarios 4 (LVPS) and 5 (FX), a key consideration is the resumption of services within two hours following a cyber incident. On this point, the Cyber Guidance states: *"An FMI should design and test its systems and processes to enable the safe resumption of critical operations within two hours of a disruption and to enable itself to complete settlement by the end of the day of the disruption, even in the case of extreme but plausible scenarios. Notwithstanding this capability to resume critical operations within two hours, when dealing with a disruption FMIs should exercise judgment in effecting resumption so that risks to itself or its ecosystem do not thereby escalate, whilst taking into account that completion of settlement by the end of day is crucial. FMIs should also plan for scenarios in which the resumption objective is not achieved. Although authorities recognize the challenges that FMIs face in achieving cyber resilience objectives, it is also recognized that current and emerging practices and technologies may serve as viable options to attain those objectives. Furthermore, the rationale for establishing this resumption objective stands irrespective of the challenge to achieve it."*

Steps for authorities—resilience of the ecosystem

An FMI is often the central hub of the financial system, and as per the Cyber Guidance, *"an FMI should take an integrated and comprehensive view of the potential cyber threats it faces. In particular, an FMI's cyber resilience framework should consider how the FMI would regularly review and actively mitigate the cyber risks that it bears from and poses to its participants, other FMIs, vendors, vendor products and its service providers,*

which are collectively referred to an FMI's ecosystem". A cyber incident can have a material impact on the broader financial ecosystem, given the interconnectedness of the system, and therefore it is essential that steps are taken that strengthen the resilience of the overall ecosystem.

Authorities should consider these key principles when strengthening the resilience of the ecosystem: (i) collective strategic planning and collaboration; (ii) identification and mapping; (iii) situational awareness; (iv) cyber threat intelligence; (v) information sharing; (vi) incident reporting; and (vii) authorities' response framework.

Collective strategic planning and collaboration

The financial ecosystem is comprised of a complex arrangement of financial entities that are interconnected and different authorities that regulate, oversee, and supervise them. During a significant cyber incident, that spreads throughout the system as showcased in this paper, it is essential that there are clearly defined arrangements between all the relevant stakeholders (public and private) to manage it. This may entail developing, ex-ante, sound collective governance structures, a strategy for managing a systemic cyber incident, clear allocation of roles and responsibilities in the sector, and strong public-private partnerships. In operationalizing these structures and approaches, authorities may put in place memoranda of understanding (MOUs) and data sharing agreements. The strategy should set out the approach that all the relevant stakeholders would take, to work collectively together in a collaborative manner, to manage the crisis which includes crisis management protocols, incident response arrangements, public communication strategies to handle the crisis and minimize panic, and business continuity arrangements.

The stress scenarios indicated that the two most significant impacts arose from cyber incidents implicating a systemically important financial institution in Scenario 2 (Bank) and a CSP in Scenario 3. Whilst the financial institution in Scenario 2 (Bank) is likely to be regulated and supervised, the CSP in Scenario 3 is likely to sit outside the regulatory perimeter in most jurisdictions. This highlights the importance of collective strategic planning and collaboration, as a sound strategic approach should include both regulated and unregulated entities that are systemically important to a financial system. In these scenarios, if the authorities develop robust processes to engage with financial institutions and their service providers, ex-ante, with clearly defined roles and responsibilities, they are more likely able to manage an incident that has the potential to become systemic. This necessitates having clear communication lines between operators of FMIs, overseers, banking supervisors, financial institutions, and service providers.

Identification and mapping

FMIs have a broad range of participants and external stakeholders (e.g. service providers) within an interconnected ecosystem. The weakest link in the chain can trigger an incident that can propagate through the system and cause financial instability. Therefore, developing a cyber mapping of interconnections can allow identification of critical nodes and help determine transmission channels through the system. Analyzing financial, operational and technological interconnections across the sector will help identify potential systemic risks from interconnectedness and concentrations. Assessing interconnectedness of the financial system network is essential to understanding how a shock to one supervised entity/service provider can spread to others. Identification of key nodes in the financial system—for example, payment and settlement systems, financial entities that carry out key services such as clearing and the technology systems underpinning them—could be done to understand cyber risk at a system-wide level. The mapping of the financial sector network can be used to estimate the impact of a cyber-attack on any of the nodes.

In order to do this, authorities are well placed to identify the different stakeholders in the ecosystem; determine how they are operationally connected; develop a mapping of the system; analyze the map to identify the critical nodes and transmission channels; and thereafter consider steps that can be taken to reduce concentration risk or build processes to manage potential systemic risk – e.g. crisis communication protocols, recovery arrangements, etc. The process to develop this map requires consistent data submissions, and strong collaboration and coordination with other authorities, regulators and market participants.

In Scenarios 2 (Bank) and 3 (CSP), mapping the financial institution and CSP to the broader ecosystem would highlight that they are critical nodes to the overall system, and therefore enable authorities to: identify threats and their impact on the sector; develop a range of different scenarios that could threaten the sector(s) on a systemic level and develop mitigation strategies accordingly; conduct scenario-based tests or stress testing based on cyber scenarios; and improve incident response capabilities. The mapping would also highlight the necessity to include the critical service provider in exercising, incident response protocols and information sharing.

Situational awareness

According to the Cyber Guidance, *"Situational awareness refers to an entity's understanding of the cyber threat environment within which it operates, and the implications of being in that environment for its business and the adequacy of its cyber risk mitigation measures".* Strong situational awareness can make a significant difference in the entity's ability to pre-empt cyber events or respond rapidly and effectively to them. A key means of achieving situational awareness for an entity and its ecosystem is: having robust threat intelligence processes; active participation in information-sharing arrangements and collaboration with trusted stakeholders within and outside the industry; and an effective cyber incident reporting framework. Authorities are well placed to catalyze initiatives to improve a sector's overall situational awareness.

Cyber threat intelligence

Authorities should require financial entities to establish a process to gather and analyze relevant cyber threat information. The analysis should be in conjunction with other sources of internal and external business and system information to provide business-specific context, turning the information into usable cyber threat intelligence that provides timely insights and informs enhanced decision-making by enabling the financial entity to anticipate a cyber attacker's capabilities, intentions and modus operandi.

An entity should be able to gather and interpret information about relevant cyber threats arising from its participants, service and utility providers and other FMIs, and to interpret this information in ways that allow it to identify, assess and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards in its systems.

In Scenarios 2 (Bank) and 3 (CSP), the entities were subject to a denial of service and ransomware attack, respectively. In both cases, having strong threat intelligence about the potential modus operandi of cyber attackers may have improved their chances of preventing the attack.

Information sharing

Cyber information and intelligence is any information that can help an entity identify, assess, monitor, defend against and respond to cyber threats. Examples of cyber information and intelligence include indicators of compromise (IOCs), such as system artefacts or observables associated with an attack; motives of threat actors; tactics, techniques and procedures (TTPs); security alerts; threat intelligence reports; and recommended security tool configurations.

By exchanging cyber information and intelligence within a sharing community, entities can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats they may face. Using this knowledge, members of the community can make threat-informed decisions regarding defensive capabilities, threat detection techniques and mitigation strategies. By correlating and analyzing cyber information and intelligence from multiple sources, an entity can also enrich existing information and make it more actionable (e.g. by sharing effective practical mitigations). This enrichment may be achieved by independently confirming the observations of other community members, and by improving the overall quality of the threat information. Entities that receive and use this information and intelligence impede the threat's ability to spread and subsequently raise their individual level of protection. Authorities should encourage financial entities to participate actively in information-sharing groups and collectives, including cross-industry, cross-government and cross-border groups to gather, distribute and assess information about cyber practices, cyber threats and early warning indicators relating to cyber threats. Multilateral information-sharing arrangements should be designed to facilitate a sector-wide response to large-scale incidents. In many jurisdictions, such information sharing networks are still not in place, and the authorities can play a pivotal role in catalyzing these initiatives through public-private partnerships, designing the information sharing frameworks, rules, platforms and media of exchange. By impeding the potential contagion of threats, the community acts in the public interest by supporting the safe and sound operation of the financial system as a whole.

In Scenarios 2 (Bank) and 3 (CSP), if the financial institution and CSP are part of information sharing networks, they would either receive ex-ante actionable intelligence to prevent an attack or they would be able to share vital intelligence with other market participants to prevent others from suffering a similar attack. During a cyber-attack, the ability to share such intelligence is vital to reduce the impact of an incident on the broader ecosystem, and authorities play a crucial role in enabling such information sharing amongst the community.

Incident reporting

Efficient and effective response to and recovery from incidents is essential to limiting related financial stability risks. Incident reporting is considered one of the primary mechanisms used by financial authorities to maintain visibility of disruptions occurring with their regulated entities, and in line with their individual mandates. Having a robust and comprehensive cyber incident reporting framework in place facilitates authorities to intervene and manage a cyber incident that has potential systemic impact.

A sound cyber incident reporting framework should have standardized templates, safe communication channels between the authorities and entities, clear thresholds for reporting and clearly articulated definitions and taxonomies. Figure 4 illustrates the components of the framework.

Figure 4. Components of a Cyber Incident Reporting Framework

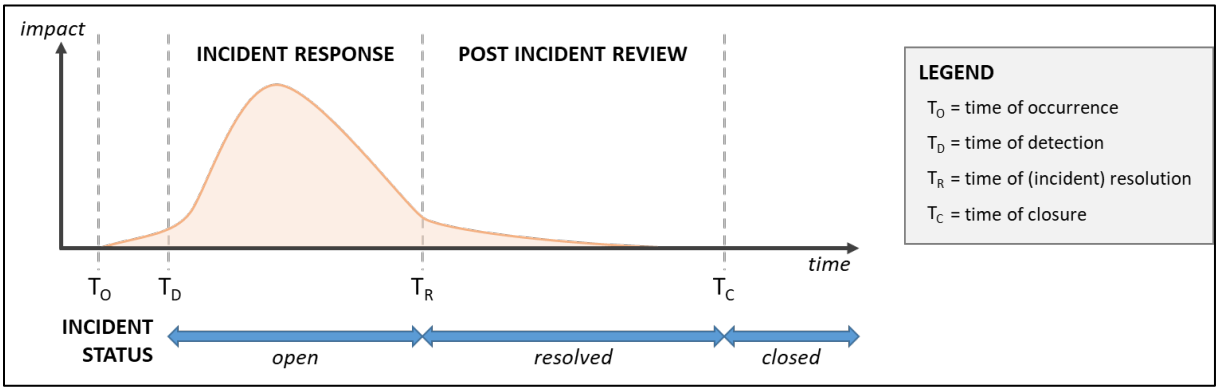
1.1 Reporting Details	1.2 Incident Details	1.3 Impact Assessment	1.4 Incident Closure
1.1.1 Reporting Entity	1.2.1 References	1.3.1 Severity Rating	1.4.1 Cause
1.1.2 Receiving Entity	1.2.2 Incident	1.3.2 Affected Parties	1.4.2 Lessons
1.1.3 Contact Details	1.2.3 Change(s) since Previous Report	1.3.3 Services and Resources	1.4.3 Supplemental Documentation
	1.2.4 Date / Time Markers	1.3.4 Impact	

Source: Financial Stability Board

Having a robust incident reporting framework, designed by financial authorities and clearly communicated to financial entities, enables all stakeholders to more effectively manage an incident (including a potentially systemic one) throughout its lifecycle.

Figure 5 shows the stages for an incident, and the most critical stage is the incident response phase, when the impact on the system could be the highest. However, restoring the services and ensuring the overall safety of the system can occur during the resolved phase too. In all cases, it is critical that entities notify financial authorities in a timely manner and keep them abreast of developments throughout, in order to ensure that the incident is being managed and not escalating to systemic levels. For this to occur, authorities should ensure that there is strong awareness amongst all entities about incident reporting and clear protocols for notification. Further, based on incident reporting, authorities should have a robust response framework in place, which dictates how they will respond in terms of crisis management at a sector level.

Figure 5. Incident Status Relative to Lifecycle State Transitions



Source: Financial Stability Board

However, whilst incident reporting is essential, it is equally important that relevant authorities are able to share incident information with each other (as long as it is legally feasible to do so).

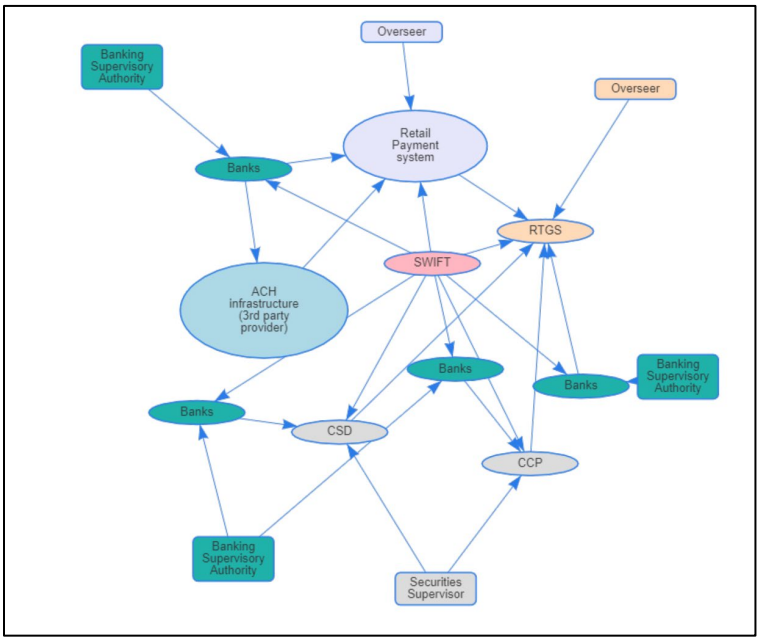
In Scenario 2 (Bank), the financial institution should have notified its banking supervisor; however, in such a situation, it is essential that the banking supervisor has sufficient protocols in place to inform the FMI operator, FMI overseer and other relevant authorities. The ability to share such crucial information in a timely manner would facilitate better incident management across the ecosystem.

In Scenario 3 (CSP), it is unlikely that the CSP is bound to reporting incidents to any financial sector authority, and there is the risk that information about the incident would only reach the authorities indirectly, leaving a time-lag to address the impact. It is therefore essential that authorities take into due consideration how to enable free-flowing sharing of incident information between authorities and invite CSPs to notify them of incidents, in a timely manner, to enhance as best as possible the incident response protocols. In some jurisdictions, there may be some critical infrastructure agencies or Computer Emergency Response Teams (CERTs) that are notified of incidents and manage incident response on a cross-sectoral basis, which may include CSPs within scope. In such cases, it is important that the financial authorities liaise with such agencies and CERTs through appropriate ex-ante arrangements and protocols.

Authorities' response framework

Although each financial system is unique and differs in its construct and stakeholders, a traditional financial ecosystem is complex and comprised of many stakeholders that are interconnected and interdependent, and this accentuates the need for a common Authorities' Response Framework (ARF). Figure 6 illustrates a traditional financial system:

Figure 6. Traditional Financial System



Source: Authors.
Note: ACH—Automated Clearing House; CSD—Central Securities Depository; CCP—Central Counterparty; RTGS—Real-Time Gross Settlement; SWIFT—Society for Worldwide Interbank Financial Telecommunication.

A financial system will be made up of an RTGS system, other types of FMIs, banks, CSPs, overseers, supervisors, and central banks. They rely on each other to provide financial and related business services within the jurisdiction and in some cases across borders. Usually, links between these financial entities work well, and are well regulated and supervised, but sometimes things can go wrong.

When things go wrong, important business services may be disrupted. Responsibility for responding to disruption sits with financial entities themselves. They will have their own methods and plans in order to react and ensure the continuity of those services. However, as financial entities rely upon one another, disruption in one part of the sector can spread to another part. It can also spread beyond the finance sector to other sectors in the jurisdiction. The authorities have a crucial role in reducing the effects of this and ensuring stable functioning of the system. This is managed through the ARF.

The ARF is a formal way for the financial authorities to co-ordinate with each other. It is used when there is an incident or threat that could cause a major disruption to financial services. The framework should be jointly owned, governed and supported by senior representation from all authorities. The framework should enable the authorities to work together to respond to an incident, whilst ensuring they consider any impacts to their own statutory objectives. All authorities have a role to play in maintaining the ARF. The ARF enables the authorities to engage and communicate with each other to respond to operational disruption in the sector. It can also be used to respond to incidents in other sectors that may indirectly affect the finance sector.

The ARF should be invoked for any operational incident that affects, or has the potential to affect, the finance sector. These incidents can have an impact on the authorities' objectives. The ARF can also be invoked for other reasons where cross-authority coordination is needed.

The ARF should operate at three levels. These are:

1. "Monitor" – The situation needs cross-authority coordination and monitoring.
2. "Engage" – The situation has worsened and needs active engagement with firms. Data gathering, relief actions and wider communications may be needed.
3. "Escalate" – The authorities' Seniors are needed to coordinate strategic action.

Authorities, when developing the ARF, should set out a playbook of scenarios and clear protocols on how to respond to the incident. This should entail four key components: (i) defining clear thresholds for an incident that requires the invocation of the ARF; (ii) processes to invoke the ARF; (iii) an incident assessment and escalation model; and (iv) a response plan and decision-making process.

The playbook, should overall, define the role of the ARF, clarify systemic-level operational incidents and systemic risk, describe how the ARF fits into the jurisdiction's financial sector crisis management, coordination and response framework, outline the ARF's activation procedure and provide guidelines for the type of information to be shared.

Given the complex setup of financial systems, as shown in this section, the ARF should aim to bring together all the relevant stakeholders (public and private) and ensure that there is clarity across the sector on how to respond to an incident that could become systemic, with clearly defined roles and responsibilities. The ARF

should be regularly tested through market-wide exercises to ensure it is effective and fit-for-purpose against a rapidly evolving threat landscape.

In Scenarios 2 (Bank) and 3 (CSP), the ARF should have been invoked to allow all the relevant stakeholders to assess the impact on the financial ecosystem, make crucial decisions, disseminate information to all market participants in a timely manner and ensure a consistency in public communications to avoid creating panic in the market.

When assessing a sector's preparedness, it is essential that financial entities have a robust CIRR framework that enables them to manage a cyber incident ex-ante and ex-post. And from the authorities' perspective, it is important that there is strong leadership to drive: collective strategic planning and collaboration; identification and mapping of the sector to identify potential transmission channels; situational awareness, which provides all stakeholders with timely actionable intelligence; and an authorities response framework, which galvanizes all parties to respond to a systemic incident in a decisive and effective manner, reducing the overall disruption to the sector.

3. Conclusions

Many authorities have a statutory mandate to safeguard financial stability where cybersecurity risk is a growing concern for macro-financial stability. While this study provided an illustrative case of Finland, the lessons are highly relevant for emerging market and developing economies. Authorities such as central banks, banking authorities, and securities regulators, have supervisory and oversight responsibilities for systemically important financial institutions and infrastructures—the critical and systemic nodes in a financial system. Many central banks also own and operate LVPSs, retail payment systems, central securities depositories, or securities settlement systems. Some also play the role of catalyst in the modernization and digitization of the banking and payment system within and across their jurisdictions. Regardless of the stage of economic development, the use of simulations for cyber stress testing exercises could assist countries to systematically evolve and achieve more mature states of cyber resilience. This paper offers two key takeaways.

First, timely systems recovery and effective queuing and liquidity risk management could generally serve as preemptive actions to reinforce cyber resilience. The scenarios selected in this paper show limited impact with practically no second round effects. This is because of the nature of the scenarios. Liquidity and settlement risks are most severe in Scenarios 2 (Bank) and 3 (CSP) when a cyber-attack hits a major bank, or several banks simultaneously through their dependence on a common CSP. The liquidity and settlement risks materialize because the incidents are assumed to last till end of day leaving no recovery potential intraday. The effects are limited to the direct effects of initial incidents without second round contagion effects. In Scenarios 4 (LVPS) and 5 (FX), it is assumed that payments affected by the incident are postponed till noon, and not removed like in Scenarios 2 (Bank) and 3 (CSP), thus leaving time for the system to recover. The results indicate a fast and full recovery in both cases. This is due to queuing and liquidity saving mechanisms of TARGET Services allowing a prompt and automated recovery.

Second, financial sector entities that have a mature CIRR framework will be best placed to respond and recover from the incident, therefore reducing the risk to the system. The identification of institutions that would need supervisory attention, in terms of ensuring they have a high quality CIRR is of great importance, as their problems could affect the system. It is therefore essential that prudential authorities work closely with their supervised entities to ensure that they have an effective, comprehensive and mature CIRR framework in place. This framework would need to encompass governance, planning and preparation, analysis, mitigation, restoration and recovery, coordination and communication, and improvement. The involvement of multiple authorities would further strengthen the resilience of the ecosystem where efforts should be made towards improving collective strategic planning and collaboration, identification and mapping, situational awareness, and the response framework.

Going forward, different kinds of forward-looking scenarios could also be envisaged and simulated for the purpose of cyber stress testing. For example, this could involve more extreme cyber-attack scenarios and different assumptions such as lengthier outages (multiple days or weeks), liquidity constraints (liquidity shortages due to collateral deterioration), net settlements (instead of real-time gross settlements), unauthorized modification of transactions, non-substitutability of settlement services, inter-day exposures (due to time zone differences involved in foreign exchange settlements), and cross-sectoral impacts (such as disruptions in capital market FMIs, or a cyber-attack on a critical infrastructure such as telecommunication networks or an energy supplier for which all financial firms depend on for their operations). These assumptions allow to test the impact of more severe scenarios. Furthermore, for internal operative purposes, the analysis could also focus on

the impact at participant levels—in addition to the system-level analysis done in this paper—to identify vulnerabilities, critical participants and counterparty exposures. This would enable the results to be observed and assessed at the participant level, particularly their exposures through first-round and second-round contagion effects. Due to confidentiality, it was not possible to present such results publicly.

Annex I. Simulation and Stress Testing Studies

Simulation and stress-testing studies on operational risks and contingency arrangements

Austria

Schmitz et al., (2006) examined operational risk and contagion in the LVPS of Austria. They analyzed three scenarios, including failure at the top transfer account, failure at the top bank, and a simultaneous failure at the three most active banks. The study also considered the stop-send rule, a function that enables an affected bank to activate a message to other participants or to the system operator with the aim of preventing the affected bank from draining liquidity at the participant (liquidity sink effect) and system levels, and thereby, reducing contagion. The study concluded that contagion effects were low under the assumption that existing business continuity arrangements were effective. For example, the affected bank had access to the information concerning its payment obligations and all payments by the affected bank were settled in time by phone, tax, or messenger service. Alternatively, the simulation results suggest that a non-negligible number of banks failed to settle payments under all three scenarios if the assumptions were less restrictive. That is, existing contingency arrangements were less than effective.

Denmark

Andersen and Madsen (2009) assessed the international best practice for business continuity arrangements in the LVPS of Denmark. The study simulated operational incidents to identify critical values associated with recovery time, critical participants, contingency measures, and the stop-sending rule. An interesting perspective is the discussion of contingency measures to handle time-critical payments, particularly foreign exchange transactions (for CLS settlement). Such measures include the use of paper-based manual procedures before the resumption of normal operations, and considerations on the capacity of staff with operational responsibilities to settle payments in the contingency mode in a timely manner to avoid disruptions to the financial system. The study also explored the use of the stop-send function.

Hungary

Lublóy and Tanai (2008) assessed the impact of operational disruptions in the LVPS of Hungary. Six scenarios were developed and grouped as full-day or part-time incidents. The scenarios differed by the number of failed participants, duration of incident, contingency procedures (back-up facilities), and the behavioral reaction of non-defaulted participants (by using stop-send rules). The study found severe disturbances in the payment system for full-day incidents without effective back-up procedures and the proportion of unsettled transactions was very high. An interesting observation was the identification of six institutions that were active money market participants in the foreign exchange swap segment. Given their relatively small balance sheets, the authors note that a liquidity shock at system-level, due to an operational incident or improper functioning of financial markets, could present a bottle neck to their balance sheets.

United Kingdom

Bedford et al., (2004) used a simulation-based approach to analyze the impact of operational incidents in the LVPS of the United Kingdom. Simulations against three scenarios were explored, including operational incidents at a single settlement bank, multiple settlement banks (simultaneously), and the core payment processing infrastructure. The UK payment system was found to be highly resilient during the simulated operational disruptions. Its robustness was attributed to the abundance of liquidity available in the system and contingency arrangements incorporated into the design of the payment system. For the latter, the RTGS by-pass mode feature enabled the possibility to revert to deferred net settlement.

Annex II. Overview of the Bank of Finland Payment and Settlement System Simulator

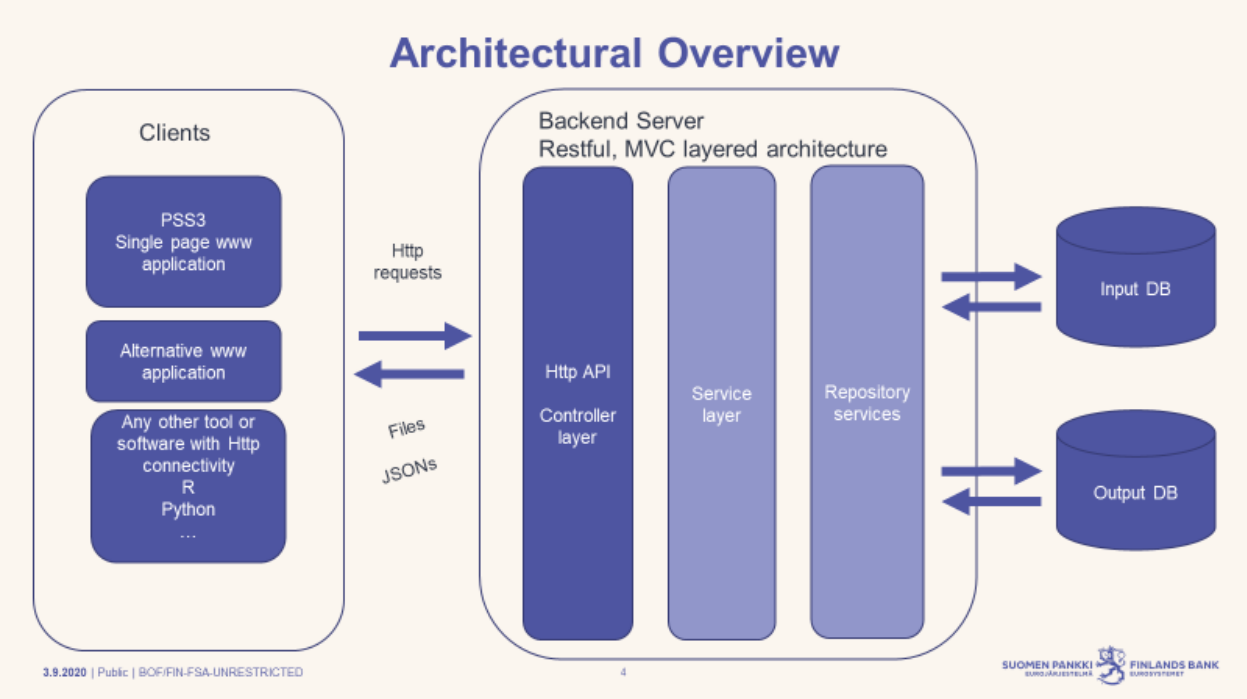
The Bank of Finland Payment and Settlement System Simulator (BoF-PSS3) is an analysis software designed for payment and settlement system simulations. The simulator can be used for studying liquidity needs and risks in payment and settlement systems. Special situations, which are often difficult or impossible to test in a real environment, can be simulated with this tool.

General architectural overview

The BoF-PSS3 simulator consists of 3 main parts:

a) A graphical user interface implemented as a web-application using mainly techniques like html and javascript.
b) A back-end server than can be installed on a regular windows PC.
c) Database storage. Currently MariaDB is used in development.

The architecture of the PSS3 program is pictured below:



Input data

In order to function, the simulator needs at least transaction data as input data. The list of the datasets that can be given to the simulator for simulations include:

- Account balances (PART)
- Transactions (TRAN)
- Intraday credit limits (ICCL)
- Bilateral and multilateral limits (BLIM) Credit caps are also supported.
- Events information (EVNT)
- Reservations (RSRV). Tailored systems only.

Usually, production data is favored but, in some cases, artificial data is also used. This would depend on the study. The simulator includes tools to import and validate these data. All the data are stored in project specific databases. The user's responsibility is to check that the input data is formally valid and then import it into the simulator. The correctness of the input data is vital. Account ids in all files must correspond to the account ids in a participant dataset.

All input data must be presented in CSV (comma separated values) format, but it can be entered in a user-defined order. The input data can be edited by exporting them from the input database as CSV files to Excel. They can then be re-imported after the changes. Older Excel versions can handle about 65,000 rows. Excel 2010 is already able to handle ~1 000 000 rows. If larger files need to be edited, other tools (e.g. Python, Matlab, R, Access or SAS) or programming is usually needed. One option is to edit the data directly in the simulator's databases with SQL-queries. The use of SQL-queries requires some moderate technical skills. In rare situations, splitting tables in sub-tables may be a suitable solution. The simulator does not include a proprietary editor for this purpose.

Simulation execution

The simulator includes tools for configuring payment and settlement system setups and running simulations. The simulator records all events and bookings. Some premade reports and statistics on simulation runs are available. The simulator allows to set up and manage settlement structures, configure settlement rules and launch, monitor and control simulation runs. The simulator keeps a log file for the user of all simulations made.

Analysis functionalities and simulation results

The simulator has functionality for reporting basic statistics for common result parameters. The output database tables contain data amongst other for the booking order of transactions and balances of settlement accounts. The input database tables contain the transactions posted to the production system, while the output tables contain the settlement flow, i.e. settlement order and timing of submitted transactions.

Users typically perform many different simulations and want to compare the results of the different runs. When the simulator's basic reports are not enough, more complex or tailored analyses may require exporting CSV files for use with tools such as Excel or other statistical software. It is thus advisable to create a structure beforehand for simulation runs and determine which results are to be stored in databases for further analysis. The databases can become overly massive when transaction volumes are high and all transaction-level events are retained in the databases. This is specifically the case when the automated stress tester is not used.

Example of supported system structures and simulation

BoF-PSS3 software supports a large variety of general system structures. It can model most of the payment and securities settlement system structures and processes found in real systems. The simulator supports real-time gross settlement (RTGS), continuous net settlement (CNS) and deferred net settlement (DNS) systems and hybrid systems. The processing options for these systems are defined by selecting appropriate algorithms. For example, QUE algorithms define how transactions are released from queues, while PNS algorithms define when and how partial net settlement of queued transactions will be invoked.

The list of central supported features include:

- RTGS, DNS, CNS
- Hybrid (combinations of the above)
- LVPS and Retail
- Delivery versus payment, payment versus payment
- Bilateral and multilateral limits (credit and debit caps)
- Multicurrency
- Multisystem
- Securities settlement systems
- Central Counterparty

The focal output factors in simulations are typically counterparty risk and overall risk, liquidity consumption, settlement volumes, gridlock situations and queuing time.

Examples of purposes the simulator

- Identify and quantify risks
- Counterparty risk
- Critical participants
- Warning indicators
- Scenario analysis
- Stress testing
- Feature prototyping
- System design
- Academic research

Examples of possible scenario types

- Participant default
- Cyber attacks
- Terror attack
- Earthquake
- Operational incidents
- Bank run
- Devaluation of collateral

- System change
- Policy change
- Mergers

Scenarios are usually generated by affecting input data and system setups in various ways. Most commonly affected factors are the following:

- Transactions (canceled, delayed, introduction order)
- Beginning of day balances
- Credit limits
- Bilateral and multilateral limits (credit and debit caps)
- System setups
- Algorithms
- Account structure

Simulations may use available data from current systems or fictional, but representative, data. The simulator can be described as a deterministic model with stochastic input.

Source: Bank of Finland
Note: Further technical details of the simulator is publicly available through the Bank of Finland's Payment and Settlement Simulator User Manual.

Annex III. Sample Questions for Cyber Exercises

As part of assessing cyber preparedness under different risk scenarios, a list of questions could be used to guide discussions in the context of tabletop-based cyber exercises. The list of questions below are guided by the components on governance, response and recovery, and testing under the Cyber Guidance (CG), where applicable.

Governance

1. What improvements could be made to the cyber resilience framework to clearly define the roles and responsibilities including accountability for decision making within the organization for managing cyber risk, including in emergencies and in a crisis? (CG, Section 2.2.6)

Response and Recovery

2. What should be included in an investigation of a successful cyber-attack? (CG, Section 6.2.1)
3. What immediate actions should be taken to contain the situation to prevent further damage and commence recovery efforts to restore operations? (CG, Section 6.2.1)
4. What judgment should be made in effecting resumption within two hours of a disruption? (CG, Section 6.2.2)
5. What should be included in a contingency plan if operations could not achieve the recovery time objective of two hours? (CG, Section 6.2.3)
6. How could an organization improve the development and testing of response, resumption, and recovery plans? (CG, Section 6.2.4)
7. What should be included in a crisis communication plan? (CG, Section 6.4.3)
8. Who are the relevant oversight and regulatory authorities that need to be promptly informed of potentially material or systemic events? (CG, Section 6.4.3)

Financial Stability

1. How many payment instructions could be left unsettled by the end of day following a prolonged outage caused by a cyber-attack?
2. What is the impact on liquidity at the system-level following a cyber-attack and their potential impact on financial markets and the real economy?
3. What is the impact on intraday liquidity risks at bank and system levels, especially for internationally active banks?
4. How could differences in time zones and settlement hours affect the impact of a cyber-attack on a cross-border multi-currency payment system?
5. Who should communicate and coordinate with whom in a cyber-attack that targets a financial entity that operates across multiple jurisdictions?

Note: The list of questions is non-exhaustive. The FSB Cyber Incident Reporting—Effective Practices for Response and Recovery provides an additional source of information to develop simulation exercises.

References

Adelman, F, J. Elliott, I. Ergen, T. Gaidosch, N. Jenkinson, T. Khiaonarong, A. Morozova, N. Schwarz, and C. Wilson. (2020). Cyber Risk and Financial Stability: It's a Small World After All, IMF Staff Discussion Note, SDN/20/07., December.

Andersen, K. S. and I. Madsen. (2009). "A Quantitative Assessment of International Best Practice for Business Continuity Arrangements in Payment Systems". In Leinonen, Harry (ed). Simulation Analyses and Stress Testing of Payment Networks—Proceedings from the Bank of Finland Payment and Settlement System Seminars 2007-2008, Scientific Monographs E:42, 17-57.

Basel Committee on Banking Supervision (BCBS) (2013a). Monitoring Tools for Intraday Liquidity Management, April.

BCBS (2013b). Supervisory Guidance for Managing Risks Associated with the Settlement of Foreign Exchange Transactions, February.

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

Chapple, M., J.M. Stewart, and D. Gibson. (2018). Certified Information Systems Security Professional, Official Study Guide, Eight Edition.

Cichonski, P, T. Millar, T. Grance, and K. Scarfone. (2012). Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology, Special Publication 800-61 Revision 2, August.

Cihak, M. (2007). Introduction to Applied Stress Testing, IMF Working Paper, WP/07/59, March.

Committee on Payments and Market Infrastructures (CPMI) (2018). Reducing the Risk of Wholesale Payments Fraud Related to Endpoint Security.

CPMI and Board of the International Organization of Securities Commissions (2022). Implementation Monitoring of the PFMI: Level 3 Assessment on Financial Market Infrastructures' Cyber Resilience, November.

CPMI and Technical Committee of the International Organization of Securities Commissions (2012). Principles for Financial Market Infrastructures, April.

Cybersecurity and Infrastructure Security Agency (CISA) (2020). Insider Threat Mitigation Guide, November.

Eisenbach, T. M., A. Kovner, and M. J. Lee. (2020). Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis. Staff Reports 909, Federal Reserve Bank of New York.

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

Financial Stability Board (2020). Effective Practices for Cyber Incident Response and Recovery, October.

Harry, C. and N. Gallagher. (2018). Classifying cyber events. Journal of Information Warfare, 17(3), 17-31.

Heijmans, R. and F. Wendt. (2020). "Measuring the Impact of a Failing Participant in Payment Systems," IMF Working Papers 2020/081, International Monetary Fund.

Hellqvist, M. and T. Laine. (ed.) (2012) Diagnostic for the Financial Markets—Computational Studies of Payment System—Simulator Seminar Proceedings 2009-2011, Bank of Finland, Scientific Monographs E:45.

Humphrey, D. (1986). Payments Finality and Risk of Settlement Failure. In Technology and the Regulation of Financial Markets, eds. Saunders, A and White, L J. Lexington Books, D.C. Heath and Company, 97-120.

International Monetary Fund. (2024). “Cyber Risk: A Growing Concern for Macrofinancial Stability”, In Global Financial Stability Report: The Last Mile—Financial Vulnerabilities and Risks, April.

Khiaonarong, T, H. Leinonen, and R. Rizaldy. (2021). Operational Resilience in Digital Payments: Experiences and Issues, IMF Working Paper WP/21/288, December.

Korpinen, K., and T. Laine. (2021). Measuring Counterparty Risk in FMIs, Bank of Finland Economics Review, Number 9/2021.

Kosse, A., and Z. Lu. (2022). Transmission of Cyber Risk through the Canadian Wholesale Payment System, Journal of Financial Market Infrastructures, Volume 10, Number 4, 1-28.

Kotidis, A and S. L. Schreft. (2022). Cyberattacks and Financial Stability: Evidence from a Natural Experiment, Finance and Economics Discussion Series 2022-025. Washington, Board of Governors of the Federal Reserve System.

Lacker, J. M. (2003). Payment System Disruptions and the Federal Reserve Following September 11, 2001, Federal Reserve Bank of Richmond, Working Paper Series, 03-16.

Laine, T. (ed.) (2015). Quantitative Analysis of Financial Market Infrastructures: Further Perspectives on Financial Stability, Bank of Finland, Scientific Monographs, E:20.

Leinonen, H. (ed). (2009). Simulation Analyses and Stress Testing of Payment Networks—Proceedings from the Bank of Finland Payment and Settlement System Seminars 2007-2008, Scientific Monographs E:42.

Leinonen, H (ed). (2005). Liquidity, Risks and Speed in Payment and Settlement Systems—A Simulation Approach, Bank of Finland Studies E:31.

Lublóy, À and E. Tanai. (2008). “Operational Disruption and the Hungarian Real Time Gross Settlement System (VIBER)”. Magyar Nemzeti Bank Occasional Papers 75, October.

McAndrews, J. J. and S. Potter. (2002). Liquidity Effects of the Events of September 11, 2001. Economic Policy Research, Vol. 8, No. 2, Federal Reserve Bank of New York.

McAndrews, J. J. and G. Wasilyew. (1995). "Simulations of Failure in a Payment System," Working Papers 95-19, Federal Reserve Bank of Philadelphia.

Schmitz, S. W, C. Puhr, H. Moshammer, M. Hausman, and U. Elsenhuber. (2006). Operational Risk and Contagion in the Austrian Large-Value Payment System ARTIS. Financial Stability Report 11, ONB, 96-113.

PUBLICATIONS

Using Simulations for Cyber Stress Testing Exercises
Working Paper No. WP/2025/085