Box 1: Cyberattacks in the CUD Large-Value Payment System and its Systemic Impact

1. Introduction

The CUD large-value payments system is an essential component of the country's payments infrastructure. This is because there is compliance with the cash leg of the obligations contracted in the financial markets (i.e., foreign exchange market, fixed income, equities, derivatives), as well as the exchange of funds between financial institutions after the multilateral net clearing of electronic payment instruments.

Payments between entities participating in the CUD are highly interconnected because the payment made by one entity is the source of liquidity for another. Thus, the inability of one entity to make its payments can, in turn, affect others, which would trigger events of a systemic nature. Moreover, if it is considered that payments made in a system such as the CUD are of a critical and urgent nature.

The growing dependence on the financial system, and in particular in financial market infrastructures, of information and communications technologies for their operation and the processing of the substantial information they handle, increases their exposure to cyber risk. This vulnerability is intensified by relying on a set of critical providers of essential services (hardware, software, electric power, and communications) for the continuous operation of the system.

According to the document Cyber Resilience for Financial Market Infrastructures published by the Committee on Payment and Settlement System (CPMI) and the Technical Committee of the International Organization of Securities Commissions (Iosco) (CPMI-Iosco, 2012), cyber risk is defined as: the combination of the probability of an event occurring within the scope of information assets, the computing and communication resources of an organization, and the consequences of that event for an organization.

According to Aldasoro et al. (2022), the most common events or methods of cyberattacks are ransomware, data theft, malware, cross-site scripting, identity theft (phishing), password decryption, and denial of service attacks. In this regard, an alternative to approach the risk of cyberattacks is through the analysis of the consequences or impact on the dynamics of payments in the CUD if its participants were victims of a cyber-attack.

Using simulations, the issue of what could happen to intraday payments made by entities if they were the subject of a cyberattack is addressed. For this purpose, and based on what was indicated by Eisenbach, Kovner, and Lee (2022a; 2022b), an individual attack typology and a massive one are taken into consideration. In the first, entities with the greatest potential for systemic impact in the CUD are selected, in accordance with the indicators of systemic importance prepared by the Financial Infrastructure Oversight Department (DSIF in Spanish) for the monitoring of financial infrastructures.[1] In the second, the criterion is the unavailability resulting from a cyberattack on the main communication service provider used by the entities to connect to the CUD. In both cases, the CUD is assumed to remain operational.

This box presents the resulting payment defaults (value and number of entities affected) from the scenarios described and also proposes a series of measures that could be considered to mitigate the risks associated with a cyberattack. Thus, provide a technical outlook that addresses cybersecurity risk and, additionally, elements that can contribute to the stability and resilience of the financial system are shared.

1 Considering the number of counterparties, quantity, and amount of transactions, as well as the role that the distributor or receiver of payments may have.

This box is organized into five sections, including this introduction. The second explains the main elements considered for the construction of simulation scenarios. The third discusses the results, emphasizing how entities not affected by the cybersecurity event could react. The fourth includes policy considerations associated with strengthening cybersecurity. The fifth section presents the conclusions and recommendations.

2. Considerations on the Design of a Cyberattack Scenario

The design of the scenarios developed here is based on the taxonomy of hypothetical cyber risk scenarios that Kaffenberger and Koop (2019) built on the Atlantic Council's (2016) proposal. According to this scheme, the scenarios can be classified into three main groups: 1) high-impact operational risk, 2) upstream infrastructure failures, and 3) external shocks and other scenarios.

The list of hypothetical scenarios related to operational risk is made up of 1) blocking malware or ransomware in a financial institution, 2) fraudulent bank transfer, 3) data breach and targeted information leakage, 4) malware in trading systems, 5) large-scale cyberattack on a global messaging network for financial transactions, and 6) simultaneous attack on systemically important institutions. The group of scenarios linked to upstream infrastructure failures includes: 1) Disruption Attack to the Central Clearinghouse, 2) disruption attack on payment processing platforms, 3) massive infection by malware, 4) cloud service provider failures, and 5) disruption of public services with domino effects. In turn, the group of external shocks includes the following scenarios: 1) cyberattack in retaliation for sanctions and 2) armed conflict.

The hypothetical scenarios implemented here to evaluate the impact that a cyberattack would have on the settlement of transactions in the CUD are framed in the high-impact operational risk and upstream infrastructure failure groups of the proposal by Kaffenberger and Koop (2019) and correspond to Table B1.1.

Table B1.1
Simulated Cyberattack Scenarios on the CUD

Simultaneous cyberattack on systematically important financial institutions	Cyberattack on communications providers
This could occur due to a blockage that would cause most of the computers of a participant in the LVPS to become unusable following malware or ransomware cyberattacks. This type of attack occurred with the Shamoon virus and the WannaCry ransomware, which significantly affected the hardware and operation of a large number of computers.	This could occur due to the blockage caused by the absence of the communication channel between the entities and the CUD, as a consequence of a malware or ransomware cyberattack on the main telecommunications provider. This, recognizing that the dependence of the financial sector, including financial market infrastructures, on electricity services and telecommunications, exposes them to risks that can impact the functioning of financial markets and economic activity.
Within Kaffenberger and Kopp's (2019) taxonomy of cyber risk scenarios, this type of attack is part of the high-impact operational risk group and specifically corresponds to hypothetical scenarios 1: of operational blocking of a financial institution through a malware or ransomware attack, and 6: of simultaneous cyberattack on systemically important financial institutions.	Kaffenberger and Koop (2019) classify this scenario within the group of upstream infrastructure failures and correspond to scenario 5: disruption of public services, causing chain effects.
This type of simulated cyberattack is similar to the one conducted by Eisenbach, Kovner, and Lee (2022a; 2022b) on the five major banks participating in Fedwire.	

Note: Financial institutions' access to the electronic Sebra services offered by *Banco de la República* (*Banrep*) can be done through: 1) Dedicated communication channels, point-to-point, between their facilities and *Banrep*, or 2) the Internet.
Source: https://www.banrep.gov.co/sites/default/files/paginas/reque_tecnico_conex_sebra.pdf.

Data: For the simulation exercise, the transactions of the ten days with the large value of payments that occurred during 2023 between 7:00 *a.m.* and 9:00 *p.m.* in the CUD were taken. Transactions between *Banrep*, the General Directorate of Public Credit and the National Treasury, and the General System of Royalties are excluded.

Reference scenario: This considers the observed transactions that were settled, one by one, in the sequence in which they occurred under the real-time gross settlement (RTGS) modality with the available beginning-of-day balances in deposit accounts of its participants during the selected dates. The value and number of successfully settled payments in this scenario are the basis for comparison to measure the impact of a cyberattack on previously formulated scenarios.

How participants react: The cyberattack scenarios described are elaborated considering that, due to the operation of the large-value payment system, the counterparties, not knowing the identity of the attacked entity (which is the one subjected to the cyberattack and stops sending payments), react differently in sending payments. Thus, in the face of the insufficient balance caused by the defaults of the attacked entity, these counterparties try to comply with the payments in the sequence of the reference scenario. However, if they are not successfully settled, their response to retry the settlement can be passive or active.

In the passive response, the affected entities (AEs), that is, those with transactions that could not settle on the first attempt, as occurred in the reference scenario, would not retry to settle them and would accumulate in a batch of defaulted transactions. Thus, the liquidity of these defaulted payments would not reach their recipient entities and would determine the size of the chain of defaults and the number of AEs in the system.

In turn, in the active response counterparties store in a queue the transactions that initially could not be settled and, to the extent that they enter resources into their account for incoming payments, they try to settle their pending queued payments using an algorithm FIFO (first in – first out). Although in this form of reaction it is also feasible to assume the lack of knowledge of the identity of the AE, the response of the counterparties makes liquidity more efficiently managed and the impacts on the value of payments and the number of entities affected are less than the resultant under a passive response.

Under each scenario, simulations were carried out where the entities reacted passively or actively to the defaults of the attacked entity, to evaluate the potential impact of the cyberattack in terms of the value and number of defaulted payments and the number of entities affected.

3. Results

3.1 Simultaneous Cyberattack on Systemically Important Entities

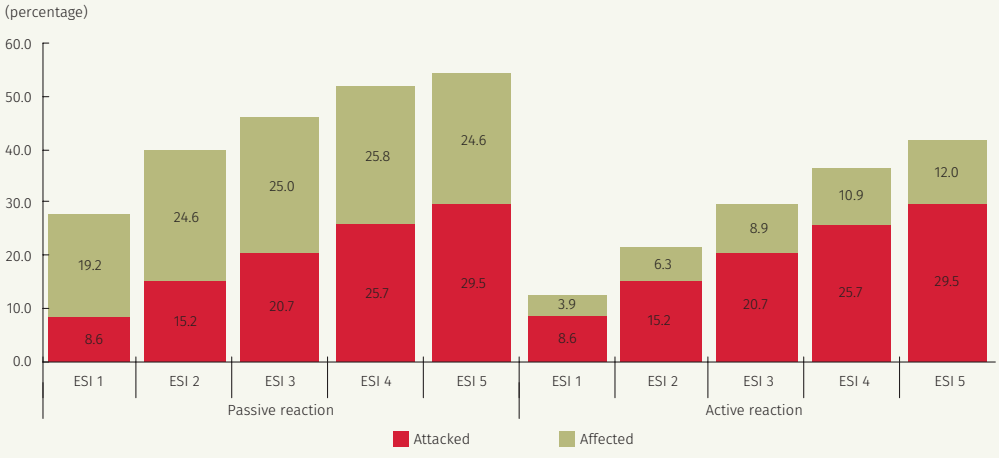
The simulation exercise, as Eisenbach, Kovner, and Lee (2022a) do for Fedwire is performed, by directing cyberattacks on up to five systemically important financial entities (ESI in Spanish) at the same time.

The selection criteria for ESI subjected to cyberattack for each of the days considered corresponds to that prepared by the DSIF to monitor the CUD. This is based on a scale of importance calculated through an analysis of major components including variables such as the number and amount of transactions carried out, the number of counterparties, as well as the role that each entity participating in the CUD may have as a distributor or receiver of payments.

Graph B1.1 exhibits the percentages of the value of payments that, concerning the reference scenario, ceased to be settled, both for the ESI subjected to simulated cyberattacks and those affected that could not comply with all their payment obligations when both a passive response and an active response are assumed.

This graph shows that when a passive response is assumed, the average value of defaulted payments, measured as a percentage of the value settled on the selected days, for the attacked ESI is between 8.6% for the main attacked ESI, to 29.5% when cyberattacks target the five most important ESI at the same time. Simultaneously, and in the same unit of measure, the average percentage of defaults of the affected entities fluctuated between a minimum

Graph B1.1
Value of Defaults as a Percentage of the Baseline Scenario: Passive and Active Reactions



Source: *Banco de la República* (DSIF).

of 19.2% when the cyberattack occurred to the main ESI, and a maximum of 25.8%, when the attack was directed to four ESI.

When affected entities are considered to take an active response, using the liquidity provided to them by their counterparties to retry the settlement of their defaulted payments, the impact on the system is significantly reduced. It can be seen in Graph B1.1 that, as the cyberattack in both the passive and active responses simulation targets the same ESI, the value of the defaults is the same. However, those of the affected entities are reduced due to the more efficient use of liquidity.

Indeed, in Graph B1.1 it is also observed that, under active response, the percentage of the default value of the affected entities is reduced in relation to the passive response. In this case, the average percentage of the value of the defaults, compared to the reference scenario, is 3.9% when the main ESI cannot send payments and 12.0% in the extreme case of a cyberattack on five ESIs.

The same Graph B1.1 exhibits that the values of defaults, measured as a percentage of observed payments (reference scenario), increase as the number of ESIs subjected to cyberattacks increases, regardless of the response assumed. It also reflects that while the defaulted payments of the attacked entities are the same, the total value of the defaults (attacked and affected entities) in the case of active response is 12.4% if it is the attack on one ESI and 41.5% if it is on five ESI. When a passive response is assumed in the simulation, the total value of defaulted payments increases to 27.7% in the event of a cyberattack on one ESI and to 54.1% when it is on five ESI.

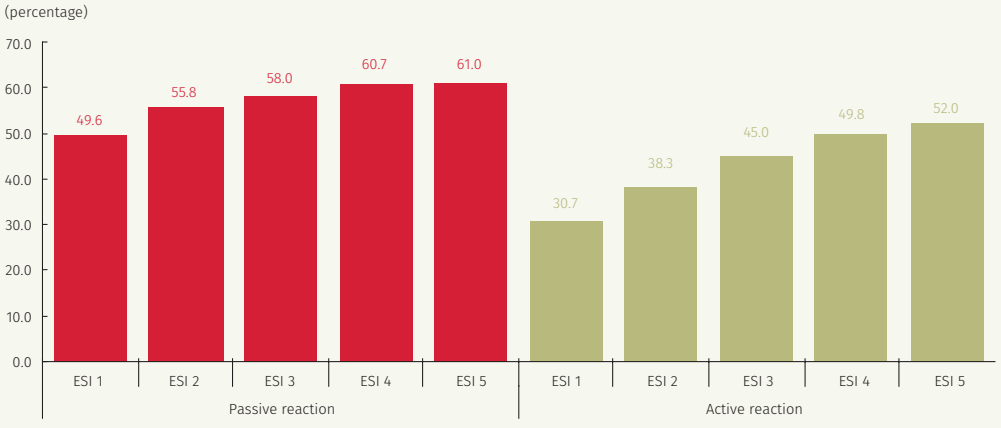
When the impact is quantified by the number of entities affected regarding the number of active ones, Graph B1.2 exhibits that by assuming a passive response in all cyberattacks (from one ESI to five ESIs), more than half (50%) of the active entities are affected; and in the extreme case of five ESIs the percentage reaches 61.0%. Under an active response, the same indicator is reduced to 30.7% for the cyberattack of an ESI, and only in the case of five ESI a little more than half of the active entities (52.0%) end up affected.

3.2 Cyberattack on Communications Providers

Cyberattacks on infrastructure service providers or their customers are classified as upstream attacks, and their knock-on effects can even impact the financial sector and the economy.

The financial sector, which includes a country's critical infrastructure, depends on electricity and the proper functioning of telecommunications and technology. Prolonged interrup-

Graph B1.2
Average Percentage of Affected Entities with respect to the Total Number of Active Ones: Passive and Active Reactions



Source: *Banco de la República* (DSIF).

tions in the operation of these providers can affect the ability of the infrastructure and its participants to operate and provide services.

One of the technical recommendations that *Banrep* makes to access the electronic services it provides,[2] as is the case of the CUD, is that its participants maintain independent alternative channels with a different provider for their connection. Thus, in the event of a contingency in which the main dedicated channel stops working, either due to an operational failure or a cyberattack, the prompt switching to the alternate channel would allow the entity to restore its connection and service as soon as possible.

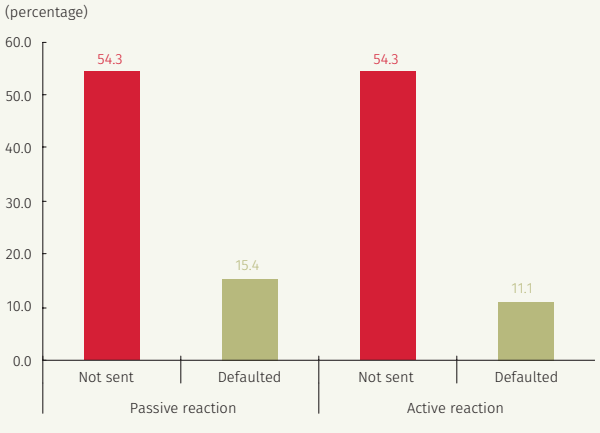
To the extent that there is a high concentration of payment system participants relying on a single telecommunications provider, the greater the impact that a cyberattack targeting this provider would cause. This situation could worsen if the entities do not comply with the recommendation to have a second line enabled.

The simulated cyberattacks here assume that entities connecting to the CUD with the primary or second telecommunications provider do not have the second dedicated line enabled and, therefore, by losing their connection, they cannot send payments.

In Graph B1.3, it is observed that, as a result of a cyberattack on the main telecommunications provider, the percentage of the value of the unsettled payments compared to those observed in the baseline scenario decreases on average by 54.3% due to the disconnection of its customers. Additionally, as a second-round effect, the default of the affected entities would be 15.4% under a passive response and 11.1% under an active response. The absence of an alternate channel, assumed in this extreme but plausible exercise, would exacerbate the potential impact of attacks on critical third parties, causing significant disruptions to the CUD.

Graph B1.4 exhibits that the cyberattack on the main provider connecting to the CUD would have a significant impact on settlement, causing the total value of defaults[3] to rise to 69.7% in the case of a

Graph B1.3
Value of Defaults due to Cyberattack on the Main Telecommunications Provider (as a Percentage of the Baseline Scenario)



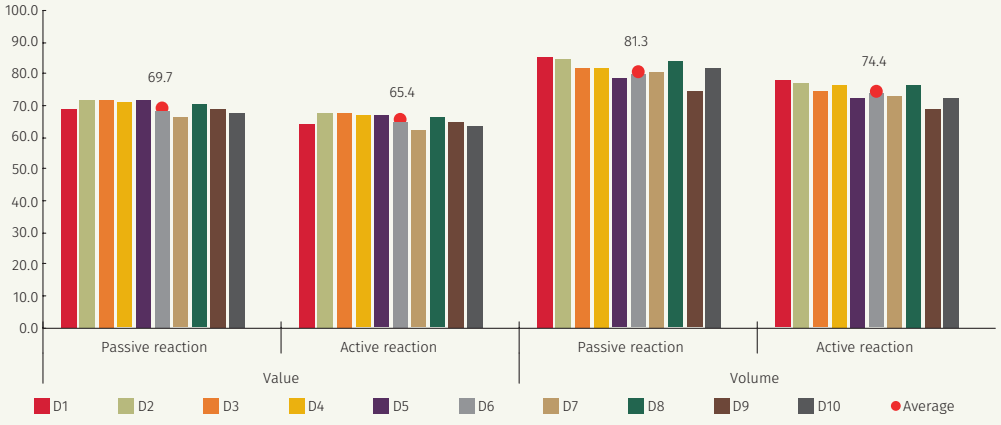
Source: *Banco de la República* (DSIF).

2 "*Requerimientos técnicos para los servicios electrónicos del Banrep Sebra*", May 2024, available at: https://www.banrep.gov.co/sites/default/files/paginas/reque_tecnico_conex_sebra.pdf

3 Both due to the direct effect of payments that disconnected entities fail to send, and as a second-round effect, payments whose counterparties use a different provider cease to be made due to the lack of liquidity received.

Graph B1.4
Value and Volume of Defaulted Payments due to the Cyberattack on the Main Telecommunications Provider

(as a percentage of observed payments in the baseline scenario)



Source: *Banco de la República* (DSIF).

passive response and only marginally reducing to 65.4% when the surviving entities react actively. Regarding the number of transactions, the cyberattack would result in 81.3% of the total transactions observed in the baseline scenario being unable to be settled under a passive response and 74.4% under an active response.

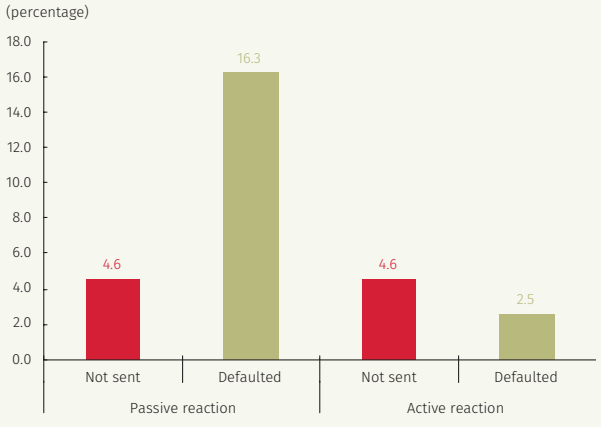
An explanation for this result is the high concentration of CUD participants in the main telecommunications provider, as shown in Table B1.2, where more than half of the active entities would be disconnected if this provider were to experience a cyberattack, preventing its clients from sending payments. Moreover, the liquidity not provided by the disconnected

Table B1.2
Percentage of Active and Affected Entities Post-cyberattack on the Main Telecommunications Provider on the CUD: Passive and Active Reactions

Day	Active post-cyberattack	Passive reaction Affected	Active reaction Affected
	As a percentage of active entities in baseline scenario	As a percentage of active post-cyberattack	
D1	50.8 %	68.9 %	65.6 %
D2	51.2 %	68.3 %	65.1 %
D3	51.6 %	68.8 %	68.8 %
D4	50.8 %	66.1 %	64.5 %
D5	50.8 %	64.5 %	64.5 %
D6	52.8 %	59.1 %	59.1 %
D7	51.6 %	60.9 %	60.9 %
D8	52.4 %	67.7 %	67.7 %
D9	53.5 %	55.1 %	55.1 %
D10	52.8 %	59.1 %	59.1 %
Average	51.8 %	64.2 %	63.4 %

Source: *Banco de la República* (DSIF).

Graph B1.5
Value of Defaults due to Cyberattack on the Second-Largest Telecommunications Provider (as a Percentage of the Baseline Scenario)



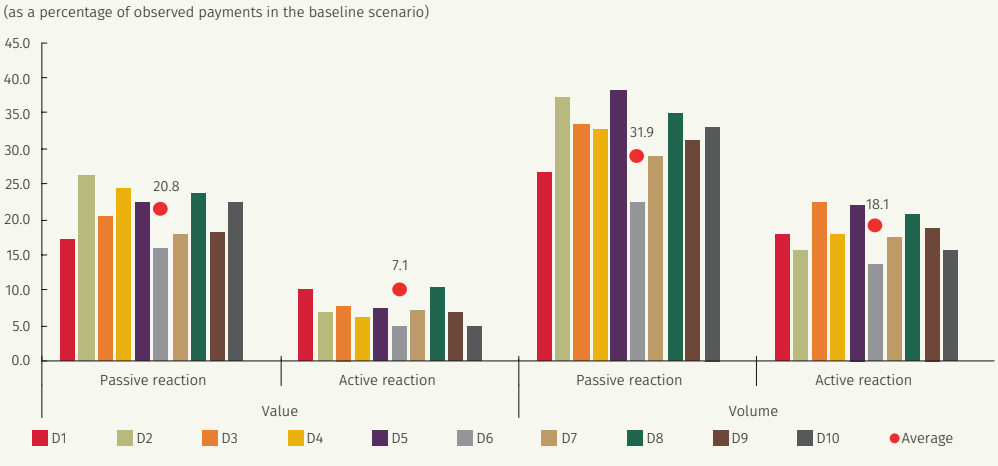
Source: *Banco de la República* (DSIF).

entities would mean that, of the surviving entities (whose connection to the system is established with another provider), two-thirds would end up affected with unsettled payments.

When a cyberattack targets the second primary telecommunications provider, which connects fewer participants to the CUD compared to the main provider, it is observed that the impact on the value and volume of unsettled payments is lower than that of the main provider. Indeed, disconnected entities would stop sending on average 4.6% of payments from the baseline scenario, and as a second-round effect, the affected entities would stop settling 16.3% of payments under a passive response and 2.5% under an active response (Graph B1.5).

Graph B1.6 exhibits that total daily and average defaults, both in value and volume, with an active response, mitigate the impact of the cyberattack compared to a passive response. Indeed, while in the passive response, the percentage of defaults concerning the baseline scenario is 20.8% in value and 31.9% in volume, under an active response, these figures decrease to 7.1% and 18.1%, respectively.

Graph B1.6
Value and Volume of Defaulted Payments due to the Cyberattack on the Second-Largest Telecommunications Provider



Source: *Banco de la República* (DSIF).

Recognizing that the number of participants connecting to the CUD is lower than that of the main provider, the direct and indirect impact of defaults generated is also reduced. According to Table B1.3, over 84% of the entities would remain active and send their payments, but 16% would cease to do so, leading to defaults by 54% of entities under a passive response and 37.3% under active response.

Given these results, it is advisable to strengthen the resilience of entities to the interruption of transactions due to the cyberattacks simulated here.

Table B1.3
Percentage of Active and Affected Entities Post-cyberattack on the Second-Largest Telecommunications Provider on the CUD: Passive and Active Reactions

Day	Active post-cyberattack	Passive reaction Affected	Active reaction Affected
	As a percentage of active entities in baseline scenario	As a percentage of active post-cyberattack	
D1	85.0 %	52.9 %	39.2 %
D2	84.6 %	57.7 %	39.4 %
D3	83.9 %	51.9 %	40.4 %
D4	84.4 %	59.2 %	36.9 %
D5	84.4 %	54.4 %	38.8 %
D6	84.8 %	45.3 %	33.0 %
D7	83.9 %	51.0 %	36.5 %
D8	83.9 %	54.8 %	40.4 %
D9	84.5 %	45.9 %	35.8 %
D10	84.8 %	51.9 %	33.0 %
Average	84.4 %	52.4 %	37.3 %

Source: *Banco de la República* (DSIF).

Diagram R1.1
Mitigation Mechanisms and Policies

- Regulatory framework and mitigation policies
- International cooperation
- Continuous education and training
- Simulation and scenario analysis
- Adoption of generative AI as a mitigation mechanism

Source: *Banco de la República* (DSIF).

4. Mitigation Mechanisms and Policies

The financial sector faces a growing cyber risk due to its interconnectedness and dependence on telecommunications providers. In addition to being a technical concern, cybersecurity has become an essential strategic priority to guarantee the stability and resilience of the global financial system. As shown in the *Financial Infrastructure Report* (2023), implementing robust policies and strategic recommendations is vital to mitigate this risk and its potential systemic impact. Among the mechanisms and policies identified to mitigate cyber risk and its potential systemic impact are (see Diagram B1.1).

- Regulatory Framework and Mitigation Policies: A robust regulatory framework is crucial to mitigating cyber risk in the financial sector. Several studies underscore the importance of developing and strengthening regulatory frameworks that promote better cybersecurity practices and adapt to evolving dynamics of threats and technologies. Additionally, fostering cooperation between the public and private sectors and harmonizing international standards is essential to improve global cybersecurity (Bank of England, 2018; BIS, 2020; Warren, Kaivanto, & Prince, 2018; Aldasoro, Gambacorta, Giudici, & Leach, 2020).
- Continuous Education and Training: Ongoing training for personnel in cybersecurity is essential to strengthen the first line of defense against cyberattacks. It is necessary to keep staff updated on the latest threats and mitigation tactics through regular drills and awareness programs. This ensures employees are prepared to properly identify and respond to cyberattack attempts (Zurich, 2014).
- Simulation and Scenario Analysis: Conducting simulations and scenario analyses is a critical tool for assessing the preparedness and resilience of financial institutions. Simulating coordinated

cyberattacks allows to identify systemic vulnerabilities and develop specific mitigation strategies. These exercises highlight the need for robust and effective business continuity and disaster recovery plans (Kaffenberger & Kopp, 2019; Eisenbach, Kovner, & Lee, 2022b).

- International Cooperation: International cooperation is essential to managing cyber risk given that cyberattacks can cross borders. The possibility of sharing threat intelligence and coordinating response strategies globally significantly improves the capacity to respond to cyberattacks and ensures a more robust defense against global threats (Aldasoro et al., 2021; BIS, 2020).

- Adoption of Generative Artificial Intelligence (AI) as a Mitigation Mechanism: Generative AI (Gen AI) comprises artificial intelligence technologies that, based on training data, can produce new and diverse content. AI introduces both opportunities and challenges[4] in cyber risk management within the financial system, including central banks (Aldasoro et al., 2024).

  In the cybersecurity field, gen AI emerges as an additional mechanism to mitigate cyber risk and its systemic impact. Among the possibilities identified by Aldasoro et al. (2024) that gen AI offers concerning cybersecurity are: 1) improved threat detection, 2) automation of routine cybersecurity tasks, 3) rapid and efficient response improving the ability to respond to cyberattacks, 4) continuous learning and adaptation of gen AI systems to emerging threats, 5) reduction in the likelihood of human error in cybersecurity threat management, 6) the possibility of creating customized behavior and risk profiles that improve the accuracy of security measures, and 7) facilitation of anticipation and neutralization of potential threats before they materialize (Diagram B1.1).

In summary, integrating gen AI into cybersecurity strategies not only strengthens existing capabilities but also introduces new ways to manage and mitigate cyber risk, reducing its potential impact on the financial system and improving systemic resilience.

5. Conclusions

- The supervisory authority can encourage CUD participants, and especially those entities that play a significant role in such infrastructure, to maintain sufficiently robust cybersecurity systems to reduce their vulnerability to cyberattacks and thus mitigate the potential negative impact of payment defaults that would arise in the system, given the interconnectivity of payments.

- It is essential to continue encouraging CUD participants to have two independent dedicated alternate channels with different providers to ensure that, in the event of a main provider failure, a rapid recovery of connection and operation is achieved through prompt switching to the alternate channel. A mechanism that could be considered by the industry, which would contribute to mitigating the impact on the system's liquidity from a cyberattack on communications providers, is to strive for moderate concentration levels in these providers. The negative impact of such an attack could be exacerbated if participants do not have an alternate channel and rely solely on a highly concentrated provider.

- Regarding how entities react to payment defaults by their counterparts, simulations conducted validate the mitigating effect obtained through more efficient liquidity use when reattempting payments by adopting an active response. The results obtained under these assumptions in the simulations aim to raise awareness among participants about how institutions can respond to payment defaults by their counterparts.

- Financial infrastructures are essential for the proper functioning of the financial system. The provision of their services is highly dependent on a high technological component, which makes them particularly vulnerable to cyberattacks. It is important to have good

4 Aldasoro et al. (2024) identifies that with the sophistication of gen AI tools and their expanded use, the frequency, speed, and complexity of cyberattacks increase. Specific threats associated with gen AI include social engineering, zero-day attacks, and malware attacks for data infiltration.

coordination between the industry and the supervisory authority to implement robust cyber resilience frameworks and well-defined response and recovery plans to ensure the continuity of critical services during and after an attack (IMF, 2024).

- Cybersecurity also plays a fundamental role in financial stability as cyberattacks can lead to direct financial losses and loss of confidence in the financial system, potentially resulting in massive withdrawals of deposits, asset liquidation, and adverse market reactions. Measures aimed at facilitating the implementation of a national cybersecurity strategy, effective regulation, adequate supervision of this risk, as well as consolidating a cybersecurity workforce, establishing national and international information-sharing agreements, and international cooperation, would strengthen the cyber resilience of the financial sector (IMF, 2024).
- Incorporating a cybersecurity component into liquidity indicators would allow financial institutions to better assess their response capacity to cyber incidents to ensure the continuity of their operations, thereby contributing to financial stability. Along these lines, the IMF's (2024) practical proposal to evaluate the potential effect of cyber incidents on banks' liquidity position consists of calculating the deposit withdrawal rate at which the liquidity coverage ratio would fall below the regulatory requirement of 100%.

References

Aldasoro, I.; Doerr, S.; Gambacorta, L.; Notra, S.; Oliviero, T.; Whyte, D. (2024). "Generative Artificial Intelligence and Cyber Security in Central Banking," *BIS Paper*, No. 145 (May), Bank for International Settlements.

Aldasoro, I.; Frost, J.; Gambacorta, L.; Whyte, D. (2021). "Cyber Risk in the Financial Sector," Bank for International Settlements.

Aldasoro, I.; Gambacorta, L.; Giudici, P.; Leach, T. (2020). "Operational and Cyber Risks in the Financial Sector," Bank for International Settlements.

Atlantic Council (2016). "Understanding Systemic Cyber Risk," Global Agenda Council on Risk and Resilience, World Economic Forum (WEF), *White Paper* (October)

Bank of England (2018). "The Bank's Approach to Operational Resilience."

Bank of International Settlements [BIS] (2020). "Principles for Operational Resilience and Cyber Risk", Bank for International Settlements.

Banco de la República (2023). Recuadro 4: Altos niveles de ciberresiliencia como factor clave para la estabilidad de las infraestructuras financieras", *Financial Infrastructure Report*, Financial Infrastructure Oversight Department (DSIF).

Eisenbach, T. M.; Kovner, A.; Lee, M. J. (2022a). "Cyber Risk and the U.S. Financial System: A pre-Mortem Analysis", *Journal of Financial Economics*, vol. 145, no. 3.

Eisenbach, T. M.; Kovner, A.; Lee, M. J. (2022b). "When it Rains, It Pours: Cyber Risk and Financial Conditions", Staff Reports, No. 1022/June, Federal Reserve Bank of New York.

International Monetary Fund [IMF] (2024) "Cyber risk: a growing concern for macrofinancial stability" – Global financial stability report: The Last Mile: Financial Vulnerabilities and Risks. Chapter 3, International Monetary Fund. (April)

Kaffenberger, L.; Koop, E. (2019). "Cyber Risk Scenarios, the Financial Systems and Systemic Risk Assessment," Cyber Policy Initiative Working Paper Series *Cybersecurity and the financial systems*, No. 4, September, Carnegie Endowment for International Peace.

Warren, G.; Kaivanto, K.; Prince, D. (2018). "Could a cyber-attack cause a systemic impact in the financial sector?", *Quarterly Bulletin*. Bank of England. (2018 Q4)

Zurich (2014). "Beyond Data Breaches: Global Interconnections of Cyber Risk," *Risk Nexus* (April).