# Box 2: Indicator of Cybernetic Risk

**Mariana Escobar Villarraga**
**María Fernanda Meneses**
**Eduardo Yanquen***

The increasing digitization of financial services has increased the system's exposure to cyber-attacks. This could compromise the security of the information, its operability and, therefore, its stability. The materialization of a cyber-risk event that affects the payment system could disrupt the flow of transactions, and this would affect confidence in the system and might trigger events that are even more serious for the stability of the financial system such as bank runs. Although the occurrence of these risks has currently been limited, the continuous monitoring and measurement of the entities' exposure represents both a challenge and a necessity for both international and local competent authorities.

This box presents the methodology for calculating the cyber risk indicator (CRI), which is one of the indicators monitored by *Banco de la República* to measure this risk and analyze its results for the entities that make up the Colombian financial system with information as of 15 March 2023. In the next *Financial Stability Reports*, this indicator will be included in the risk analysis for the Credit Institutions (CI). The box is divided into four sections: the first presents the perspectives and occurrence of some recent cyber risk events and their international and local monitoring; the second describes the CRI and the methodology for its calculation; the third presents the data and its analysis; and the fourth corresponds to the conclusions.

## 1. International and local cyber risk monitoring

The materialization of cyber risk events has shown the importance of this issue.[1] Recent attacks on central banks such as the hacking of the Central Bank of Denmark's website in January of this year (Reuters, 2023) and the attack on more than thirty government entities in Costa Rica including the Ministry of Finance in April 2022 led the latter country to take measures and declare a state of emergency. In this context, the Committee on Payments and Infrastructure Markets (CPIM) and the International Organization of Securities Commissions (Iosco) (Central Banking, 2023) recently warned about vulnerabilities in key global financial infrastructures. This is in addition to reports published by the Financial Stability Board (FSB), the International Monetary Fund (IMF), and the Bank for International Settlements (BIS).

Because of the above, cyber risk has gained importance as a systemic risk in the analysis of the financial system. At the international level, the Systemic Risk Barometer survey, which was developed and implemented by the Depository Trust and Clearing Corporation (DTCC, 2023) and collects information from U.S. and foreign entities, ranked cyber risk as the third most important since it was chosen by 47.0% of the respondents as very relevant for 2023.[2] Likewise, the Systemic Risk Survey done by the Bank of England in the first half of 2023 placed cyber risk second in importance only to geopolitical risk when it was cited by 75.0% of respondents as the one that, if it materialized, would be among the most damaging to the UK financial system and by 9.7% as their main concern (Bank of England, 2023). Fur-

---

* The authors are members of the Financial Stability Department (DEFI). We would like to thank the Information Security Department of *Banco de la República* and Daniela Vargas, intern at the DEFI, for their support in the preparation of this box.

1 For the financial system, the main risks related to cybersecurity include ransomware, malware, attacks on web platforms, and phishing, etc.

2 The first risk chosen by respondents as "very relevant" was geopolitical along with trade tensions while the second was inflation.

thermore, there are other indicators such as the global cybersecurity index (GCI) published by the United Nations International Telecommunication Union (2023), which presents, by member country, the strengths and opportunities for improvement in the monitoring of cyber risk. In the GCI ranking, Colombia ranked 81 out of 183 in the most recent report with data as of 2020.[3]

In contrast, at the local level, the results of the Survey of Perception of Financial System Risks, developed by *Banco de la República* (2023), show an increase in the number of entities that consider cyber risk to be one of the five risks which would have the greatest impact on the financial system if they occurred.[4] However, its share remains low (2.8% in the December 2022 version). Furthermore, the compromise of the information systems of a health company at the end of last year set off alarms in the country.

The Office of the Financial Superintendent of Colombia (FSC) issued two documents, External Circular 007/2018 and External Circular 033/2020 which provide instructions on the minimum requirements for cybersecurity risk management and guidelines for reporting metrics and incidents related to information security and cybersecurity, respectively. In addition, the FSC published the Box "Measuring maturity in operational risk management in banking entities," in which it analyzes the level of maturity of the entities with respect to the adoption of policies to combat cyber risk in January 2023. Furthermore, the Banking Association of Colombia (Asobancaria) has a Security Incident Response Team (CSIRT, 2023) that is responsible for fostering collaboration among its members and the exchange of information to effectively deal with cyber threats in addition to providing periodic refresher courses.

## 2. Scoring Methodology

The CRI is calculated with information provided and collected by the company Security Scorecard.[5] Data from ten factors that represent different dimensions of cyber risk is used for its construction. These are aggregated by a weighted average where the weight of each factor is determined by Security Scorecard using machine learning techniques and is categorically illustrated as high, medium, and low (Diagram B2.1). The CRI has a scale of zero to one hundred where a score of one hundred indicates that no cybersecurity issues were detected at the time of the measurement, and a score of zero indicates that multiple issues have been detected that could compromise the security of the assessed entity.

## 3. Analysis of the score

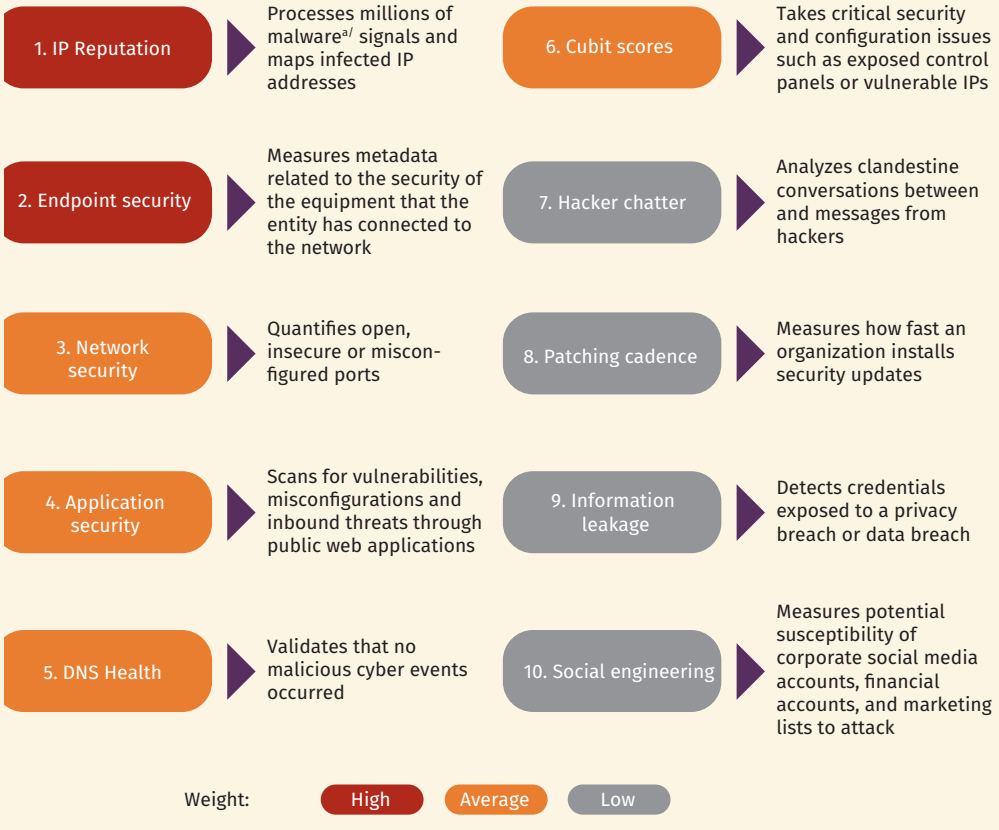
In its function of ensuring the stability of the financial system, *Banco de la República* considers it relevant to monitor the measures taken by credit institutions to protect themselves against cyber risk. The factors that make up the CRI and the overall CRI rating given by Security Scorecard are used to determine the level of protection the entities have. When the rating of each of the factors that make up the CRI is analyzed, the components that show the greatest variation in the case of banks are endpoint security and IP reputation. The former was the lowest rated for this sector in November 2022 (Graph B2.1). This means that a percentage of the equipment used by these types of entities is exposed and should be subjected to security checks. Factors such as the cubit score, hacker chatter and network security have excellent ratings throughout the year. Nevertheless, the performance of factors such as patching cadence, which has been consistently decreasing throughout the

3 According to the publication (International Telecommunication Union, 2023), the country showed strength in the technical indicator, which measures the implementation of technical strategies by national and sector-specific entities, and opportunities for improvement in the organizational indicator, which measures national and organizational cybersecurity strategies.

4 The two main risks mentioned by the entities in the survey are: deterioration in Colombia's economic outlook and materialization of credit risk.

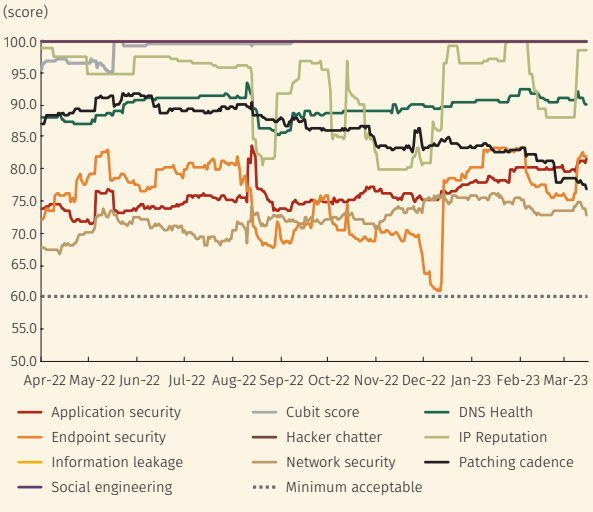
5 Security Scorecard is an information security company that rates cybersecurity positions through threat analysis for third-party management and IT risk management purposes.

Diagram B2.1
Cybersecurity Indicator Modules




a/ Malware is a term for any malicious software created to damage or exploit vulnerabilities in information networks, services, or devices.
Acronyms: *Domain Name System* (DNS) *Internet Protocol Address* (IP).
Source: *Security Scorecard*.

Graph B2.1
Cybersecurity Factors of the Banks



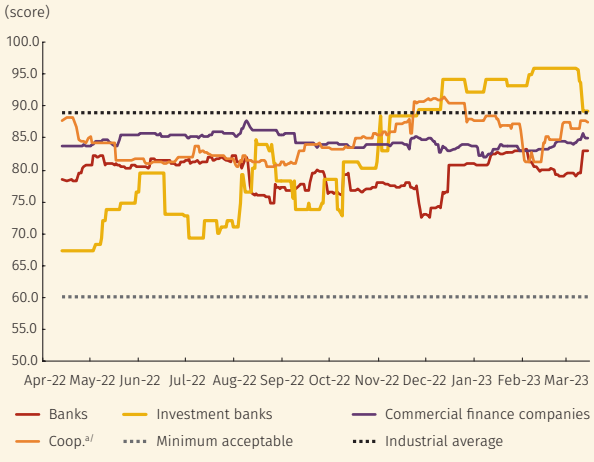

Source: *Security Scorecard*; calculations by *Banco de la República.*

year and in the latest measurements has a score of 76.8 points, is the lowest performing factor after network security which is in the last position with 72.9 points.

To construct the CRI by type of entity, the rating given to each entity by the Security Scorecard was taken. The individual figure was weighted by the share of assets of the respective institution within its reference group, and the average was calculated with this data. For banks and cooperatives, the total number of entities that make up these groups was considered while for investment banks (IB) and financing companies (FC), the entities that represent 92.4% and 78.9% of the assets, respectively, were taken into account due to the availability of information.

First of all, the most volatile CRI and, at the same time, the one that has shown the greatest improvement over the last year and gone from 67.4 to 89.2 points, is the one corresponding to the FCs and is currently the best among the CIs. This increase has been driven primarily by improvements in endpoint security and DNS health factors. There have been variations in the CRI for banks and cooperatives, but it has remained stable over the last year; However, it is important to pay attention to the lowest rated factors for banks (Graph B2.2), as this sector is currently the one with the lowest CRI in the system. Last of all, the rating for the FCs has remained relatively stable over the

Graph B2.2
Weighted Average of Rating by Type of Entity




a/ Financial cooperatives
Source: Security Scorecard; calculations by *Banco de la República.*

past year. These data are around the average rating of the financial services industry which, according to Security Scorecard data, was 88 points as of the cut-off date.

## 4. Conclusions

Cyber risk monitoring continues to evolve and gain importance. At the local level, the CRI used by *Banco de la República* makes it possible to measure the status of the policies and measures implemented by the entities in the Colombian financial system. The most recent CRI figures show that all the factors used to calculate it have a score above 70 points which indicates that the entities are managing their cyber risk well, especially the CFs who have improved their indicators significantly. However, indicators such as network security and endpoint security could be strengthened As for the CRI by type of entity, all of them are above 80 points. This indicates that the financial system has taken the necessary steps to protect itself against cyber vulnerabilities.

## References

*Banco de la República* (2023) *Encuesta de percepción sobre riesgos del sistema financiero*, January. Accessed on 28 April 2023 at https://repositorio.banrep.gov.co/handle/20.500.12134/10592

Bank of England (2023). "Systemic Risk Survey Results, 2023 H1", accessed on 28 April 2023 at https://www.bankofengland.co.uk/systemic-risk-survey/2023/2023-h1

Central Banking (2023). "CPMI and IOSCO Raise 'Serious' Concern Over Cyber Security Flaw", accessed 28 April 2023 at https://www.centralbanking.com/central-banks/financial-stability/fmi/7953859/cpmi-and-iosco-raise-serious-concern-over-cyber-security-flaw

CSIRT (2023). "¿Quiénes Somos?", Asobancaria, accessed on 28 April 2023 at https://csirtasobancaria.com/quienes-somos

DTCC (2023). "Systemic Risk Barometer Survey", accessed on 28 April 2023 at https://www.dtcc.com/-/media/downloads/Systemic-Risk/Systemic-Risk-2023

International Telecommunication Union (2023). *GCI Fourth Edition Report*, accessed on 28 April 2023 at https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Reuters (2023). "Hackers Hit Websites of Danish Central Bank, Other Banks", accessed on 28 April 2023 at https://www.reuters.com/technology/denmarks-central-bank-website-hit-by-cyberattack-2023-01-10/