SOUTH AFRICAN RESERVE BANK

Draft directive in respect of cybersecurity and cyber-resilience within the national payment system

Directive No. 02 of 2023

Contents

1. Definitions

1.1 In this directive,

1.1.1 **cloud computing** means a model for enabling convenient, on-demand network access to a shared pool of configured computer resources (e.g. a network, servers, storage facilities, applications and other services) that can be provisioned and released rapidly with minimal management effort or service provider interaction;

1.1.2 **compromise** means a violation of the security of an information technology (IT) system;

1.1.3 **cyber-event** means any observable occurrence in an information system. Cyber-events sometimes provide an indication that a cyber-incident is actually occurring;

1.1.4 **cyber-incident** means a cyber-event that adversely affects the cybersecurity of an information system and/or the information that the system processes, stores or transmits, or which violates the security policies, security procedures and/or acceptable use policies, whether resulting from malicious activity or not;

1.1.5 **cyber-resilience** means the ability of a payment institution to continue carrying out its mission by anticipating and adapting to cyber-threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber-incidents;

1.1.6 **cyber-risk** means the combination of the probability of cyber-incidents occurring and their impact;

1.1.7 **cybersecurity** means the preservation of confidentiality, integrity and availability of information and/or information systems through the

cyber-medium. In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved;

1.1.8 **cyber-threat** means a circumstance with the potential to exploit one or more vulnerabilities that adversely affects cybersecurity;

1.1.9 **data breach** means a compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, data transmitted, stored or otherwise processed;

1.1.10 **multi-factor authentication** refers to the use of two or more authentication factors to verify a user's identity;

1.1.11 **payment institution** refers to persons designated, authorised, registered or regulated under the National Payment System Act 78 of 1998 (NPS Act), including but not limited to clearing system participants, settlement system participants, third-party payment providers and system operators;

1.1.12 **operator** means an operator of a payment system, including payment clearing house system operators, operators of settlement systems and the operator(s) of payment system financial market infrastructures (FMIs);

1.1.13 **vulnerability assessment** means a systematic examination of an IT system, including its controls and processes, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.

2. Background

2.1 In terms of section 10(1)(c) of the South African Reserve Bank Act 90 of 1989, as amended (SARB Act), the South African Reserve Bank (SARB) is required to perform such functions, implement such rules and procedures, and, in general, take such steps as may be necessary to establish, conduct, monitor,

regulate and supervise payment, clearing and settlement systems. Furthermore, the NPS Act provides for the management, administration, operation, regulation and supervision of payment, clearing and settlement systems in the Republic of South Africa, and for connected matters. The power to perform the functions as provided in the SARB Act and the NPS Act are performed by the National Payment System Department (NPSD) within the SARB. The SARB plays an important role in ensuring the safety, efficiency and resiliency of the national payment system (NPS).

2.2 The NPS encompasses the entire payment process, from payer to beneficiary, and includes settlement between banks. The process includes all the tools, systems, instruments, mechanisms, institutions, agreements, procedures, rules or laws applied or utilised to effect payment. The NPS is a primary component of the country's monetary and financial system as it enables the circulation of money and assists transacting parties to make payments and exchange value.

2.3 In terms of section 12 of the NPS Act, the SARB is empowered to issue directives, after consultation with the payment system management body, to any person regarding a payment system or the application of the provisions of the NPS Act. Currently, in terms of section 3 of the NPS Act, the Payment Association of South Africa is recognised by the SARB as a payment system management body to organise, regulate and manage its members in the payment system.

2.4 The payment landscape has evolved significantly over the past two decades, with digitisation, financial technology (fintech), automation and artificial intelligence (AI) changing the manner in which payments are effected. The rapid growth in digitisation and automation has introduced alternative payment solutions that are faster, more cost-effective and more efficient. However, these technologies also increase IT security risk and cyber-risk in the NPS as payment institutions become more dependent on computer networks and third-party IT service providers. This requires an increased level of resilience against cyber-incidents, as cyber-attacks on IT infrastructures, particularly

those that are critical, could lead to a disruption that might develop into systemic events in the NPS, thus impacting negatively on the soundness, integrity, safety and efficiency of the NPS.

2.5 The cyber-environment exposes payment institutions as well as payment, clearing and settlement systems to potential operational, legal and reputational risks, including business interruptions, data loss, fraud, breach of privacy and network failures, which may result in financial losses. Cybersecurity and cyber-resilience contribute positively to the operational resilience of payment institutions as well as payment, clearing and settlement systems and payment system FMIs, and further contribute to the overall resilience of the broader NPS.

2.6 The resilience of payment institutions, operators as well as payment, clearing and settlement systems will minimise disruptions within the NPS and contribute to maintaining the confidence of consumers in payment services. Furthermore, it is vital that payment system FMIs, as essential platforms in the NPS, are also secure from, and resilient to, cyber-threats and cyber-attacks. A lack of security controls and recovery from cyber-attacks may lead to low levels of cybersecurity protection and the failure to settle obligations in the settlement system by the end-of-value date, trigger a systemic event and/or cause financial instability.

3. Purpose

3.1 The SARB, acting pursuant to its powers in terms of section 12 of the NPS Act, hereby issues this directive to impose cybersecurity and cyber-resilience requirements on payment institutions; payment, clearing and settlement systems; payment system FMIs; and operators within the NPS.

4. Application of this directive

4.1 This directive applies to payment institutions, including designated clearing system participants; third-party payment providers; system operators; operators of payment clearing and settlement systems; and payment system FMIs.

5. Directive

5.1 Payment institutions and operators must develop and maintain cybersecurity and cyber-resilience frameworks that include the following:

5.1.1 Cyber-governance

5.1.1.1 Payment institutions and operators must have written effective cyber-governance arrangements that:

a. define the cybersecurity and cyber-resilience objectives;
b. outline the people, processes and technology requirements for protecting information systems, managing cyber-risks, and providing timely communication and effective responses to, and recovery from, cyber-attacks;
c. require the board of directors (board) or senior management of the payment institution and the operator to:
    i. determine the cyber-risk tolerance levels of the payment institution, operator or a payment system FMI;
    ii. approve the cybersecurity policies and strategy, and cybersecurity and cyber-resilience framework;
    iii. oversee the development and implementation of the cybersecurity policies and strategy, and cybersecurity and cyber-resilience framework;
    iv. ensure that there is an annual review of the cybersecurity policies and strategy, and cybersecurity and cyber-resilience framework;

v. ensure that the cybersecurity and cyber-resilience framework is aligned to the payment institution or operator's operational risk management framework and business continuity plan;
vi. ensure that the cybersecurity and cyber-resilience framework is based on industry standards and international best practices, and comply with legislative and regulatory requirements;
vii. ensure that the cybersecurity and cyber-resilience framework clearly articulates the identification of cyber-risks and the required controls to manage and mitigate the cyber-risks;
viii. ensure the appointment of a senior executive and technical experts with the relevant skills, expertise and experience accountable for cybersecurity and cyber-resilience; and
ix. ensure that the cybersecurity and cyber-resilience framework makes provision for collaboration and information sharing with the SARB and other relevant payment industry stakeholders;

d. require the senior management of the payment institution, or the operator to:
i. regularly keep the board informed and updated on the cybersecurity and cyber-resilience status of the payment institution and on any developments relating to cyber-threats within the NPS;
ii. ensure that the payment institution or the operator comply with this directive and any other applicable cyber-resilience legislation and regulations;
iii. conduct third-party risk assessments on third-party service providers prior to onboarding; and
iv. ensure that the roles and responsibilities in respect of cybersecurity and cyber-resilience are clearly outlined in agreements entered into with third-party service providers.

5.1.2 **Identification of critical operations and information assets**

5.1.1.2 Payment institutions and operators must:

a. identify critical technology, operations, processes, supporting information and assets that require protection against cyber-compromise;
b. identify internal processes, procedures, information assets and external dependencies that will strengthen their security and resilience to cyber-threats, including:
    i. the identification and ranking of technology, processes and functions in a risk-based approach to ensure that protective, detective response and recovery efforts are facilitated in a timely manner;
    ii. the identification of technology, information assets, system configurations and access rights to information assets;
    iii. the classification of processes and information assets in terms of sensitivity and criticality;
    iv. the regular review and updating of critical business processes that will ensure that information remains current and accurate;
    v. the identification of cyber-risk interconnections within the NPS; and
    vi. the identification of access rights to information assets by third-party service providers.

5.1.3 **Cybersecurity measures**

5.1.3.1. Cybersecurity frameworks must include security controls, processes and systems that effectively protect and safeguard the confidentiality, integrity and availability of services provided as well as the information handled by payment institutions or operators. These measures should, however, be proportionate to the threat landscape, risk tolerance and systemic role of the payment institution or operators in the NPS, and must include the following:

a. the embedding of protective controls that minimise the likelihood and impact of a successful cyber-attack on identified critical business functions and information assets;
b. the development and implementation of measures to protect critical and sensitive information, which should, at a minimum, include access control, multi-factor authentication (MFA) and encryption;

c. the development and implementation of protective measures to mitigate risks arising from the interconnected entities within the NPS;
d. the development and implementation of measures that mitigate cyber-risk and address anomalous behaviour by staff with access to the system;
e. the continuous training of all relevant staff to develop and maintain awareness and to ensure that staff are knowledgeable in detecting and addressing cyber-risk;
f. the development and design of cyber-secure and cyber-resilient payment instruments and services that ensure that software, network configurations and hardware supporting or connected to critical systems are tested against security standards and cyber-attacks;
g. the development and implementation of cyber-hygiene measures that include the following:
    i. ensure that access management policies and processes include strong password security controls, access rights and privileges, and periodic access reviews;
    ii. ensure that third-party service providers that have access to payment institutions or operators' information assets are subject to access restrictions and monitoring;
    iii. establish processes to manage access to privileged accounts and monitor the use of IT systems for suspicious and unauthorised activities;
    iv. implement MFA for accounts used to access payments institutions' or operators' sensitive information through the internet;
    v. ensure the implementation of MFA for access to critical systems;
    vi. ensure the implementation of network perimeter defence controls;
    vii. implement multiple layer security controls to curb the effect of security compromises;
    viii. ensure the application of security patches to address vulnerabilities of systems;
    ix. ensure that security patches are tested prior to application to IT systems;

x. ensure there are security standards applicable to software, systems and devices;
xi. develop processes to monitor the application of security standards and ensure that the standards are continually reviewed for relevance to an evolving threat landscape; and
xii. implement malware protection through defence and response mechanisms, ensuring regular scanning of information assets for malicious activities;

h. the development and implementation of data security measures that include the following:
i. data loss prevention policies – which should include measures that will enable the payment institutions or operators to detect and prevent the unauthorised access and transmission of sensitive data;
ii. ensuring the encryption of data storage systems and endpoint devices to protect sensitive data; and
iii. ensuring that IT systems that are managed by third-party service providers are protected and subject to security standards.

5.1.4 **Detection**

5.1.4.1. Cyber-resilience frameworks must include cyber-attack trigger points and detection measures to continuously detect and monitor anomalous events and activities. The cyber-attack detection measures must include the following:

a. multi-layered trigger indicators and detection controls that accommodate processes, people and technology, ensuring that each layer serves as a safety net;
b. incident response processes to ensure that there is efficient recovery from incidents that could not be prevented; and
c. security measures that identify and facilitate the analysis of irregular behaviour by persons with access to the payment institution or operator's information assets and network.

5.1.5 **Response and recovery**

5.1.5.1. Payment institutions or operators must have arrangements in place designed to enable the resumption of critical operations safely and swiftly, including:

a. early detection of cyber-attack attempts and/or successful cyber-attacks and immediate initiation of recovery efforts to restore operations;
b. the design and testing of systems to enable the resumption of critical operations within the following time frames:
    i. two (2) hours for payment, clearing and settlement systems and payment system FMIs;
    ii. as per the timelines specified by the payment system management body (PSMB) for the payment institutions that are members of, registered or authorised by the PSMB; and
    iii. as per the timelines specified by operators for payment institutions that participate in such systems, which shall not exceed eight (8) hours of recovery/resumption time for all payment institutions;
c. ensuring that there are adequate measures in place to enable the return and resumption of critical operations within two (2) hours for payment, clearing and settlement systems and payment system FMIs; within the timelines specified by the PSMB for the payment institutions that are members of, registered or authorised by the PSMB, or as per the timelines specified by operators of payment, clearing and settlement systems for payment institutions that participate in such systems, which shall not exceed eight (8) hours of recovery/resumption time for all payment institutions;
d. compliance with payment and settlement obligations to minimise the likelihood of a systemic event;
e. planning for extreme scenarios, including an analysis of critical functions and interdependencies to prioritise resumption and recovery actions in a contingency mode while remedial efforts are in progress where the resumption of critical operations may not be possible within two (2) hours;

f. developing and testing response, resumption and recovery plans on a quarterly basis;

g. continuous update of plans based on information sharing, current cyber-threat intelligence and information from previous cyber-events; and

h. the inclusion of third-party management plans in their cyber-resilience frameworks to provide for the following:

   i. extensive due diligence to evaluate the cyber-resilience measures that relevant third parties have in place*;*

   ii. an assessment of the criticality of processes that may be outsourced prior to entering into envisaged outsourcing contracts;

   iii. obtaining independent security attestation reports from third parties as an additional layer of assurance of the security posture of the third-party service providers; and

   iv. ensuring that the business continuity plans of critical third-party service providers align with the objectives and policies of the payment institution or operator.

i. in the event of outsourcing to a cloud service provider (CSP), ensuring that the following principles are adhered to:

   i. the payment institution or operator shall conduct due diligence on the CSP;

   ii. the payment institution shall identify, monitor and mitigate any jurisdiction risk relating to the data transmitted, stored and processed in the cloud; and

   iii. the payment institution shall remain accountable for the data stored and processed, and for the overall security and resilience of the solutions developed on the cloud.

5.1.6 **Testing**

5.1.6.1. Payment institutions or operators must develop and implement cyber--resilience testing programmes and methodologies which include the following:

a. different test scenarios and simulations of various cyber-attacks;
b. penetration testing on systems and processes through the simulation of cyber-attacks on their systems with relevant stakeholders, including critical service providers in order to identify the vulnerabilities in their systems;
c. testing of systems after implementation of significant system changes to identify any security vulnerabilities due to a system change; and
d. regular vulnerability assessments that enable the identification and assessment of security vulnerabilities in the systems.

5.1.7 **Information sharing**

5.1.7.1. Payment institutions or operators must:

a. include access, collection and the sharing or exchange of information with external stakeholders in the cybersecurity and cyber-resilience frameworks;
b. plan arrangements for information sharing through trusted channels;
c. participate in information-sharing groups and organisations such as the Cybersecurity Hub and Computer Incident Response Teams to assist the payment institution or operator in gathering, distributing and assessing information about cyber-practices, cyber-threats and early warning indicators relating to cyber-threats;
d. ensure that information-sharing arrangements comply with the Protection of Personal Information Act 4 of 2013 and/or any other applicable data protection legislation, and that the personal data of clients of payment institutions or operators is protected and not compromised during the information-sharing process; and
e. ensure that information-sharing arrangements comply with relevant provisions of the Cyber Crime Act 19 of 2020 relating to the disclosure of information.

5.1.8 **Situational awareness**

5.1.8.1. Payment institutions or operators must:

a. understand the cyber-threat landscape of the environment within which they operate, and the adequacy of their risk mitigation measures;
b. develop cyber-threat intelligence processes that include gathering and analysing cyber-threat information to identify the potential impact of cyber-threats on their institution or systems and promote cyber-situational awareness; and
c. ensure that the scope of the cyber-threat information gathering process includes the collection and interpretation of information about cyber-threats arising from other NPS participants, to enable the identification of cyber-threats emanating from other participants and the development of relevant detection, protection and recovery measures.

5.1.9 **Learning and evolving**

5.1.9.1. Payment institutions or operators must:

a. ensure that cybersecurity and cyber-resilience frameworks are adaptive and evolve with the dynamic nature of cyber-risk, to identify, assess and manage security threats;
b. ensure continuous learning from previous cyber-incidents and events to ensure that their security systems are improved to increase resilience;
c. keep abreast of new cyber-risk management processes and continually monitor technological developments that effectively counter existing and emerging forms of cyber-attacks; and
d. include predictive and anticipatory capabilities that go beyond reactive controls and include proactive protection against future cyber-events in the risk management practices.

5.2 **Cyber-incident reporting requirements**

5.2.1 Payment institutions or operators must immediately report material cyber-incidents to the SARB and provide the SARB with a report within 24 hours of the cyber-attack. The report must include the:

a. date and time of the incident;
b. cause and source of the incident;
c. type and nature of the incident;
d. impact on the provision of services;
e. expected recovery period;
f. impact on stakeholders;
g. improvement action plan;
h. possible systemic effect of the incident on other payment institutions or operators; and
i. any other information as may be requested by the SARB relating to the cyber-incident.

6. Inspection

6.1 The SARB may conduct an independent inspection on payment institutions; operators or payment system FMIs in the form and manner determined by the SARB to establish compliance with this directive by payment institutions or operators.

6.2 Payment institutions or operators must produce to the SARB officials all documents or information relevant for this directive upon request by such officials.

6.3 In case of suspected non-compliance, the SARB officials may seize documents and records relevant for this directive from the affected party.

7. Effective date and non-compliance

7.1 This directive will be effective 90 days after its publication. The SARB reserves the right to amend any requirements in this directive.

7.2 Payment institutions or operators must comply with the requirements or conditions as stipulated in this directive.

7.3 Contravention of this directive is an offence in terms of section 12(8) of the NPS Act.

8. Conclusion

8.1 Any enquiries or clarification concerning this directive may be addressed to the following email address: NPSDIRECTIVES@resbank.co.za.