भारतीय रिजर्व बैंक

RESERVE BANK OF INDIA

www.rbi.org.in

CONFIDENTIAL

DOS.CO/CSITEG/S8149 /31.01.015/2023-24 January 19, 2024

To

The Chairman/Managing Director/Chief Executive Officer
Scheduled Commercial Banks (excluding Regional Rural Banks);
Local Area Banks; Small Finance Banks; Payments Banks;
Primary (Urban) Co-operative Banks;
Non-Banking Financial Companies;
Credit Information Companies; and
All India Financial Institutions (EXIM Bank, NABARD, NaBFID, NHB and SIDBI)

Madam/Dear Sir,

Guidelines on reporting of unusual cyber incidents - Revised

Please refer to "Guidelines on reporting of Unusual Cyber Security Incidents" issued in September 2020. Regulated Entities (REs) are required to report unusual cyber security incidents including certain IT incidents to the RBI as per the aforementioned guidelines.

2. While it is essential for REs to follow incident reporting guidelines to ensure timely reporting and effective risk mitigation, certain concerns have been observed in the incident reporting process. These concerns include:

a) REs are not reporting the incidents in a timely manner (within 6 hours of detection, unless explicitly mentioned otherwise) and/ or inordinately delaying their response to queries raised by Cyber Security and IT Risk Group (CSITEG) over the incident reporting portal (DAKSH portal) subsequent to reporting of the incident.

b) Some of the REs (who are already onboarded on DAKSH portal) are reporting the incidents over email instead of reporting in the DAKSH portal.

c) Additionally, REs are not reporting incidents of downtime when the downtime window surpasses the prescribed threshold as per extant requirements.

d) Also, there have been instances where RBI is made aware of cyber incidents through media and other channels, rather than directly by the RE through the available reporting framework.

e) Recent incidents of card data leakage pertaining to various REs have led to apprehensions about whether such incidents must be reported by the REs irrespective of number of cards and related details.

f) Often, REs are not reporting incidents occurring at their vendor/ partners/ Third Party Service Providers (TPSPs). Compromise of information assets or disruption of services due to cyber incidents at the vendor/ partner/ TPSPs has a contagion effect on the entities receiving services from such entities leading to disruption of customer services.

g) REs, at times, are not updating relevant fields in DAKSH portal. For example, the following discrepancies are generally observed resulting in "incompleteness" in incident reporting.

S.No.	Field Name	Issues observed
1.	Description of Incident	The narration is vague whereas it should sufficiently describe the incident
2.	Current status of Resolution of the incident	Not updated and shown as "unresolved" despite RE resolving the incident
3.	CAPEC-ID, CWE-ID	Not provided, wherever available also
4.	Financial loss, Amount involved in incident (either resulting into loss or otherwise)	Either not updated or reporting in absolute value rather than in ₹ lakh
5.	Root Cause Analysis (RCA)	Not updated and shown as "Yet to be ascertained" despite RE submitting RCA
6.	Whether Communicated to CERT-In, LEAs, IBCART, affected customers	Status is not updated after action is taken (as applicable to the incident type)

3. In order to address the above concerns and proactively adapt the guidelines according to the recent developments in cyber landscape, revised guidelines, to be followed by the REs with regard to reporting of unusual cyber incidents are given under **Annex** below.

4. REs shall review their incident management process to align the same with regulatory expectations. The procedures for incident assessment and reporting shall be updated and followed to ensure that the RE is: (a) able to understand and assess the characteristics of reportable cyber incidents; (b) the incident management and reporting team are sufficiently trained to report the cyber incidents to RBI in accordance with the extant requirements set out in these guidelines; and (c) the concerns highlighted in para 2 above are addressed effectively.

5. This shall come into effect from February 1, 2024. A copy of the same shall be placed before the Board of Directors in its ensuing meeting.

6. Please acknowledge receipt.

Yours faithfully,

(T.K. Rajan)
Chief General Manager

Encl: As above.

Annex

Guidelines on Reporting of Unusual Cyber Incidents

Definitions[1]

Cyber - Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.

Cyber event – Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring.

Information System - Set of applications, services, information technology assets or other information-handling components, which includes the operating environment and networks.

Cyber security - 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.

Cyber-attack - Malicious attempt(s) to exploit vulnerabilities through the cyber medium to damage, disrupt or gain unauthorized access to assets.

Information Asset[2] - Any piece of data, device or other component of the environment that supports information-related activities. Information Assets include information system, data, hardware and software.

Cyber incident[3] - shall mean a cyber event that adversely affects the cyber security of an information asset whether resulting from malicious activity or not.

Data Breach - 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] Source – FSB Cyber Lexicon (updated in April 2023) unless explicitly mentioned otherwise.

[2] Information Asset definition is adapted from "Guidance on cyber resilience for financial market infrastructures" June 2016 publication of Bank for International Settlements and International Organization of Securities Commissions

[3] Cyber incident definition is adapted from FSB Cyber Lexicon (updated in April 2023). By the definition, it includes cyber security as well as IT incident.

Regulatory Expectations

1. REs[4] are advised to report (means initial reporting) the unusual cyber incidents to the RBI, positively within **six hours of detection** of the cyber incident. *Initial reporting or "notification" within six hours of detection should aim to contain a minimal set of available information which may then be supplemented by more comprehensive updates.*

2. REs are advised to mandatorily report the cyber incidents only on the DAKSH portal (https://daksh.rbi.org.in). Those entities (some of the UCBs and NBFCs) who are yet to get access to/ "onboarded onto" DAKSH portal, may, in the interim, continue to report over email[5]. However, they shall also write to DAKSH@rbi.org.in for onboarding and subsequent reporting, follow-up of the incident on DAKSH portal. Once onboarded onto DAKSH portal, the REs should not report over email thereafter.

3. REs shall respond to queries raised by CSITEG on DAKSH portal **within five working days**, unless the RE has mentioned specific timeline for submitting the inputs sought. REs shall provide all necessary details, as available, in their responses to the queries raised. Further, REs shall ensure to keep CSITEG updated on the developments related to the incident reported and submit relevant information, if any, over DAKSH portal. This is in addition to responding to the specific queries raised by CSITEG.

4. REs should strive to submit Root Cause Analysis (RCA) report at the earliest possible time from the date of detection of the incident. The time required for finalising the Root Cause Analysis (RCA) report may vary, contingent on the nature of the incident. In cases where no external audit or forensic investigation is necessitated, it is imperative that the RCA report be submitted to RBI within **10 working days from the initial detection of the incident.** The RCA should clearly describe (**as per the applicability and availability of the information**) the type of incident, the root cause of the incident, the lapses observed, the threat/ attack vector, the threat actor, the chronological order of action taken by the RE after the occurrence of the incident, lessons learnt, remedial actions taken/ proposed for preventing such incidents in the future.

[4] Indian banks should also report unusual cyber incidents affecting their overseas operations.

[5] cybersecurityucb@rbi.org.in for UCBs and cybersecuritynbfc@rbi.org.in for NBFCs.

5. Wherever additional time is necessary (depending upon the incident), REs should provide a timeline for submission of RCA/ action planned **within 10 working days from the date of initial detection of the incident**.

6. REs shall update all relevant fields while reporting/ updating the incident. REs shall mandatorily update the status in DAKSH portal immediately on resolution of the incident. Further, wherever relevant, REs should strive to provide attack pattern [CAPEC-ID - Common Attack Pattern Enumeration and Classification] based on https://capec.mitre.org/index.html and Related weaknesses [CWE-ID – Common Weakness Enumeration] based on http://cwe.mitre.org/data/index.html in the incident description.

7. Unavailability of systems/ services or cyber-attacks or unusual cyber incidents at the Third-Party Service Providers (TPSPs) / Vendors/ Partners may lead to, among other things, significant disruption of customer services at the REs' end. There is an increased risk of systemic effect due to cyber-attacks at such TPSPs/ Vendors/ Partners providing services across multiple REs. Hence, REs are advised to mandatorily report any unusual cyber incident at Vendor/ Partner/ TPSPs' infrastructure which impact their operations. REs shall ensure that cyber incidents are reported by the service provider without undue delay, so that the incident is reported by the RE to the RBI within 6 hours of detection by the Vendor/ Partner/ TPSP.

8. Cyber Incident types that are required to be reported

a. **Unusual Cyber Incidents:** This could be, for illustrative purpose, one/ more of the following types of incidents but not necessarily limited to:

(i) Malware, Ransomware attack;

(ii) Data/ customer information/ business information breach;

(iii) Malicious traffic observed from bank's information system to a suspicious IP/ Command & Control terminal (or) any other internal/ external information system;

(iv) Denial of Service (DoS) / Distributed Denial of Service (DDoS) attacks exceeding 30 minutes;

(v) Customer service disruption (Beyond a threshold time limit as discussed below)

(vi) Exploitation of vulnerabilities resulting into compromise of integrity of the system/ application. (e.g., Parameter manipulation/man-in-the-middle type of incidents);

(vii) Email phishing, spoofing attacks leading to execution of fraudulent transactions;

(viii) Website defacement;

(ix) Any other type of cyber incident not necessarily falling into one of the above.

b. Instances wherein deficiencies in the RE's or TPSP's or in any of the entity in the payment ecosystem's (e.g., payment aggregator, payment gateway, payment system operator) internal systems/ applications/ processes (including reconciliation exercise associated with payment ecosystem) results into wrongful credit/ debit to the RE/ customers/ others amounting to ₹30 lakh[6] or more. **Illustrative but not exhaustive list of such instances are –**

(i) Instances of compromise of authentication factors, exploiting the loopholes in CBS to put through unauthorised transactions in Savings/ Current account or internal GLs.

(ii) Transactions due to Application logic defect/ technical glitches/ patching deficiencies/ incorrect setting of parameters/ flags; process defects; database maintenance/ configuration/ patching deficiencies; connectivity problem/ timeout issues; deficiency in authentication/ authorisation mechanism; parameter configuration/ validation issues; scalability and/ or performance limitations in application/ database/ network layers.

(iii) Excess credit/ debit in settlement process in payment ecosystem for unauthorised transactions.

c. Significant phishing / vishing attacks on customers, if found having similar modus operandi as well as timespan or any other common features like geographic region, (e.g., customers of same/near-by branches defrauded etc), resulting in wide impact having reputational risk for the RE (or) amount involved

[6] Such limit in the amount involved is kept only to relatively exclude incidents of lesser value for reporting to CSITE Group under the "unusual" category. Notwithstanding the quantum of amount involved, the REs shall be responsible to take necessary action that are required to protect its customer interest and safeguard its reputation.

exceeding ₹ 50 lakh[7]. **Here, the RE shall report within 24 hours as soon as they are able to detect the incident meeting these criteria.**

d. Isolated incidents of significant cyber-attacks (including but not limited to Phishing/Vishing/Social Engineering etc) on customers involving even a single customer shall be reported if the amount involved exceeds ₹ 50 lakh[8].

e. Card Skimming incidents, if any common modus operandi/pattern of attack is identified across many ATM sites/ geographical area, **or** the amount involved in the incident is more than ₹10 lakh, or new modus operandi identified etc.

f. Leakage of card data **(or)** card data exposed in the public domain/ dark web only if total number of cards exceeds 1000[9] in one instance (or) cumulatively total number of cards exceeds 1000 in multiple instances in a week. Also, it shall be reported, only if the RE is able to clearly establish that:

(i) details of card data (card number, expiry date/ CVV) leaked are sufficient to put through a card not present transaction and/ or

(ii) details leaked (partial card data/ BIN number along with customer details) establish that card/ customer data belong to them[10].

g. **Downtime Reporting**

Significant levels of customer service disruptions due to non-availability of IT systems of the RE (irrespective of whether it is managed by the RE or its TPSP) must be reported[11]. The “significant” down time limit is given only for reporting under unusual cyber incident and has no relevance in determining the RTO (Recovery Time Objective).

The reporting requirement is as follows:

(i) For those REs with a monthly mobile banking transaction volume of 10 crore or more[12], the reporting criteria is:

[7] --as given the above foot note --

[8] --as given in the above foot note --

[9] The threshold is provided only for reporting purpose. Notwithstanding the number of records involved, the REs shall be responsible to take necessary action that are required to protect its customer interest, ensure financial stability and safeguard its reputational risk.

[10] For example, in the leaked data, if only BIN number belongs to the RE and no other data available belongs to the RE’s customers, **then such instance is not required to be reported.**

[11] Irrespective of whether it is planned or unplanned downtime. Though planned downtime is not a cyber incident, due to the customer service disruption, it is required to be reported in the incident reporting module of DAKSH portal. REs are encouraged to report planned downtime proactively even before the scheduled activity, if it is expected to breach the threshold.

[12] Refer to latest available monthly data (https://www.rbi.org.in/Scripts/NEFTView.aspx) in RBI data releases on “Bankwise Volumes in NEFT/RTGS/Mobile Transactions/Internet Banking Transactions”. While mobile banking

For Unplanned downtime

I. Beyond 30 minutes of downtime between 8 am and 8 pm (or)

II. Beyond 2 hours of continuous downtime.

For Planned downtime

Any planned downtime activity where the downtime window is more than 8 hours.

(ii) REs not falling in the above category given in 8.g.(i), the reporting criteria is:

For Unplanned downtime

I. Beyond 2 hours of downtime between 8 am and 8 pm (or)

II. Beyond 4 hours of continuous downtime.

For Planned downtime

Any planned downtime activity where the downtime window is more than 8 hours.

h. **Customer Service Degradation or High Transaction Failures**

Significant levels of customer service disruptions occur due to system performance issues and/or non-availability of critical intermediate systems[13]. In such scenarios, the information systems downtime may not, at times, be even continuously breaching the thresholds discussed in the para 8.g above for incident reporting. However, such issues due to performance degradation and/ or non-availability of information systems of the RE (irrespective of whether it is managed by the RE or its TPSP) must still be reported[14] as unusual cyber incident, if any of the below criteria is met:

(i) high technical decline (of more than 3%) in digital payment transactions in a day;

(ii) non-availability of services at branches (say, for example, due to CBS non-availability/ unable to access CBS/ connectivity issues etc.,), for more than 2 hours, if the service is disrupted at least across 20% of the branches (or) 500 branches whichever is lower. [This scenario is not applicable for REs with less than 500 branches];

transaction volume serves as an indicative reference for differential reporting under the downtime category, REs should note that reporting is not restricted solely to mobile banking downtime.

[13] Illustratively, high Technical Decline in UPI, IMPS, AePS or any other payment systems; customers facing internet problems with internet banking/ e-commerce transactions/ services due to non-availability of 2FA application etc.

[14] Irrespective of whether the causation is due to a planned activity or otherwise.

(iii) customer service impact due to degradation of any of the key performance indicators[15] of digital banking/ payment services beyond a set threshold as defined by the RE.

REs with no retail banking function (or) foreign banks operating through branch mode with less than five branches in India are exempted from reporting under para 8.g and 8.h.

i. A major near-miss cyber-attack with the potential to escalate into an unusual cyber incident, as per RE's risk assessment.

9. **Reporting Authority**: The incidents should be reported by the CISO, or any other competent authority(ies) designated for this purpose by the RE.

10. Types of incidents/ observations that are not required to be reported under unusual cyber incident:

a. Instances of phishing/vishing type of incidents at customer end (not meeting the above given criteria).

b. Isolated instances of forged identity through V-CIP (Video based Customer Identification Process).

c. Accounting/ clerical errors (incorrect ledger posting- cr/dr) that are rectified/ reversed subsequently.

d. Security alerts/ cyber events not materialising into a cyber incident. Example – viruses, malwares, trojans, vulnerabilities that are detected and handled appropriately on an ongoing basis.

e. DoS/ DDoS attack not lasting beyond 30 minutes contiguously or not impacting the customer service/digital channels even if it last beyond 30 minutes.

f. Phishing websites, rogue apps that are monitored /brought down on an ongoing basis.

g. Branch connectivity issues (excluding the scenario discussed above).

h. Physical tampering of ATMs/ ATM sabotage (not to include skimming attacks) resulting into loss for the RE.

[15] This is applicable only for Scheduled Commercial Banks. The key performance indicators (refer Para 5 of the Master Direction DoS.CO.CSITE.SEC.No.1852/31.01.015/2020-21 on Digital Payment Security Controls dated February 18, 2021) as defined by the RE shall be referred for this purpose.

i. Skimming attempts at isolated ATM sites (with no financial loss to the banks/customers).

11. Notwithstanding the aforementioned provisions, any cyber incident (or) potential cyber incident meeting one or more of the criteria outlined below should also be reported:

a. upon determination and communication by the Reserve Bank as relevant for reporting purposes to the concerned RE;
b. poses a major reputational impact to the RE encompassing negative press/ unfavourable media coverage, social media attention.

12. Wherever there is ambiguity in the assessment of an incident for reporting purpose, REs may contact CSITE Group for necessary guidance.

****