ශ්‍රී ලංකා මහ බැංකුව
இலங்கை மத்திய வங்கி
CENTRAL BANK OF SRI LANKA

25 January 2016 | **CIRCULAR** | **Ref: 02/17/150/0095/001**

Bank Supervision Department

To: The Chief Executive Officers of Licensed Commercial Banks and
Licensed Specialised Banks

Reporting on Cyber Security Events

All licensed banks are requested to submit the reports on Cyber Security Events (CSE) as follows with immediate effect:

a. CSE-I as at Annex within one working day from the detection of any CSE.

b. CSE-II as at Annex within 15 days from the end of each quarter.

c. Details of all CSE detected by the bank from 01.01.2015 in same format as in (b.) above, if not already submitted.

The above details shall be e-mailed to dbsd@cbsl.lk or delivered in confidential cover to the Director of Bank Supervision.

Yours faithfully,

Director of Bank Supervision

Encl:

6 වන මහල, අංක 30, ජනාධිපති මාවත, තැ. පෙ. 590, කොළඹ 01, ශ්‍රී ලංකාව
94 11 2477100/659
6 ஆம் மாடி, இல. 30 சனாதிபதி மாவத்தை கொழும்பு 1
த. பெ. இல. 590, கொழும்பு 01, இலங்கை
94 11 2477711
banksup@cbsl.lk
Level 6, No. 30, Janadhipathi Mawatha, Colombo 1
P. O. Box. 590, Colombo 01, Sri Lanka.
www.cbsl.gov.lk

CSE-I

To: Director of Bank Supervision

Report on Cyber Security Events

Name of Bank:

Reporting time period:

Type of incident[a]	Summary of incident	Date of detection	Physical location/ branch (if applicable)	Estimated/actual impact of the incident (Financial and Operational)[b]	Internal reporting authority[c]	Law enforcement authorities involved (if applicable)

.....

Name and designation of authorised officer

(a) Type of incident: Intrusion/hacking, Malware, Malicious code, Virus, Phishing, Denial of service, Social engineering, Unauthorized system usage, Other (specify)

(b) Please provide the amount in case of financial impact and description in case of operational impact.

(c) To whom the event has been internally escalated.

[Email to dbsd@cbsl.lk or deliver in confidential cover to the Director of Bank Supervision.]

CSE-II

To: Director of Bank Supervision

Quarterly Report on Cyber Security Events

Name of Bank:

Reporting time period:

Type of incident[a]	Summary of incident	Time period of incident	Date of detection	Physical location/ branch (if applicable)	Impact of the incident (Financial and Operational)[b]	Internal reporting authority[c]	Involved law enforcement authorities (if applicable)

.....

Name and designation of authorised officer

(a) Type of incident: Intrusion/hacking, Malware, Malicious code, Virus, Phishing, Denial of service, Social engineering, Unauthorized system usage, Other (specify)

(b) Please provide the amount in case of financial impact and description in case of operational impact.

(c) To whom the event has been internally escalated.

[Email to dbsd@cbsl.lk or deliver in confidential cover to the Director of Bank Supervision.]