ASIAN SCHOOL OF CYBER LAWS

Cyber Security Checklist for Telecom Companies: 20 Questions to Ask

Tick each question you can answer with a confident yes. Every unticked box is a place to start.

VISIBILITY

01 ☐ Do we have a complete inventory of network devices, including software versions?

02 ☐ Do we know every system that stores SIM keys, call records and customer data?

03 ☐ Do we know every internet-facing system and API, including dormant ones?

ACCESS

04 ☐ Is phishing-resistant MFA used for administrators, contractors and cloud platforms?

05 ☐ Are network devices managed only from an isolated management network?

06 ☐ Do we require strong identity checks before SIM changes and number ports?

NETWORK

07 ☐ Are edge devices patched quickly when vulnerabilities are exploited?

08 ☐ Do we filter malicious signalling traffic from other networks?

09 ☐ Are subscriber databases and intercept systems strictly isolated?

DETECTION

10 ☐ Do we check network devices regularly for implants and unauthorised changes?

11 ☐ Would we detect large amounts of subscriber data leaving the network?

12 ☐ Do we actively hunt for state-sponsored intruders?

RESILIENCE

13 ☐ Are device configurations and critical systems backed up offline?

14 ☐ Could we rebuild core systems after a destructive attack?

15 ☐ Would emergency calls keep working during a major outage?

RESPONSE

16 ☐ Do we have a plan for evicting a sophisticated intruder with national agencies?

17 ☐ Can we replace SIMs or add protections quickly if keys are exposed?

18 ☐ Have we run a nationwide outage exercise in the last 12 months?

PEOPLE AND GOVERNANCE

19 ☐ Are store and call centre staff trained to resist SIM swap fraud and bribery?

20 ☐ Does the board treat network security as a national responsibility?