ASIAN SCHOOL OF CYBER LAWS

Cyber Security Checklist for Retailers: 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 an inventory of every connected device in stores and distribution centres?

02 ☐ Do we know which suppliers can access our systems?

03 ☐ Do we know which suppliers we can't trade without?

ACCESS

04 ☐ Do help desks, including outsourced ones, verify identity strongly before resets?

05 ☐ Is phishing-resistant MFA used for administrators and remote access?

06 ☐ Are supplier accounts limited to what they need and monitored?

NETWORK

07 ☐ Are payment systems separated from other store and corporate systems?

08 ☐ Are store devices such as refrigeration controllers kept off the public internet?

09 ☐ Have default passwords on all store devices been changed?

DETECTION

10 ☐ Do we monitor identity systems around the clock for suspicious changes?

11 ☐ Would we detect unauthorised changes to our checkout pages?

12 ☐ Do we detect customer account takeover and loyalty fraud?

RESILIENCE

13 ☐ Are backups of identity and core systems stored offline and tested?

14 ☐ Could our stores keep trading if central systems went down?

15 ☐ Could we keep goods flowing if a key supplier was attacked?

RESPONSE

16 ☐ Have we agreed who can decide to take systems offline?

17 ☐ Do we have a plan to communicate with customers during an outage or breach?

18 ☐ Have we run a ransomware exercise in the last 12 months, ideally simulating peak season?

PEOPLE AND GOVERNANCE

19 ☐ Are help desk and store staff trained to spot social engineering?

20 ☐ Does the board treat cyber risk as a risk to the ability to trade?