

# Securing Multi-Location F&B Operations in Saudi Arabia

A Systems Integrator's Guide to CCTV, Network Infrastructure &  
Data Protection



The background of the slide features five horizontal, wavy lines in a light purple color, creating a sense of movement and depth.

# 01

## Introduction

# Introduction

Saudi F&B is opening branches faster than most operators can standardize what protects them. A single-location mindset around cameras, networks, and customer data does not scale to ten locations, and it breaks down entirely at fifty.

This report separates what is actually required by Saudi law from what compliance marketing implies is required — the surveillance camera law that names food service establishments directly, the personal data law that extends to footage from every one of your cameras, and the cybersecurity framework that isn't legally required for most F&B operators, though it's worth knowing which vendors hold themselves to it anyway.

The exposure is real. It is also more specific, and more manageable, than most operators assume.

The background of the slide features several horizontal, wavy lines in a light purple color, creating a sense of movement and depth against the dark grey background.

# 02

## Operational Risk Landscape

## — SECTION 02

# Operational Risk Landscape

Retail and hospitality businesses are targeted at a scale most multi-branch F&B operators underestimate.

### INCIDENTS & CONFIRMED BREACHES, 2024

#### Retail

**837** incidents

**419 confirmed breaches**

Up from 725 incidents in 2023

#### Accommodation & Food Service

**211** incidents

**48 confirmed breaches**

Source: RH-ISAC / Verizon DBIR 2025, Retail & Hospitality Industry Insights



### NAMED CASE STUDY · OCTOBER 2022

A phishing and fraud campaign, documented by CloudSEK and reported via Infosecurity Magazine, targeted **KFC and McDonald's customers across Saudi Arabia, UAE, and Singapore** — fake apps and phishing sites harvesting payment card data, one-time passwords, and personal information.

**This isn't hypothetical — it's already happened to two of the region's largest F&B brands, and the pattern is still active.**

Source: CloudSEK, via Infosecurity Magazine, October 2022

### REGIONAL THREAT CONTEXT

**2,215** attacks/week ▪ **77%** via email

Middle East businesses face 2,215 cyberattacks per week on average, against 1,682 per week across EMEA. Of malicious files delivered regionally, 77% arrive by email.

Source: CheckPoint, via Security MEA, February 2025

Multi-branch F&B operations multiply the points of exposure. Every location is a camera system, a network endpoint, and a POS terminal handling customer data.

The background of the slide features several horizontal, wavy lines in a light purple color, creating a sense of movement and depth against the dark grey background.

# 03

**What Actually Applies to F&B  
Operators — and What Doesn't**

## What actually applies to F&B operators — and what doesn't

Most compliance content written for the Saudi market treats every regulation as universal. It isn't.

### **NCA Essential Cybersecurity Controls — the exclusion**

#### CHALLENGE

Most compliance content assumes every business must meet the NCA's Essential Cybersecurity Controls.



#### IMPACT

Confirmed false for F&B — ECC is mandatory only for government entities, critical national infrastructure, and named essential services (telecom, healthcare, financial services, logistics). F&B is not in scope unless individually designated. That's precisely why working with an NCA-registered partner matters here: it's not a legal requirement for your business, but it is a voluntary standard your integrator chose to meet anyway — and it's a standard most vendors serving F&B never bother with.



**Magnaite is NCA-registered. Not because F&B requires it — because we hold ourselves to it.**

📺 **MOI Surveillance Camera Law — the direct hit**

**CHALLENGE**

Royal Decree, October 3, 2022, names establishments offering food services, shopping centers, and commercial complexes explicitly.



**IMPACT**

A defined set of installation, retention, access, and penalty obligations applies directly. Detailed below.

| Requirement    | Detail                                                                                                                                                                                     |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Installation   | Cameras installed before license granted or renewed                                                                                                                                        |
| Retention      | Recordings preserved unaltered pending any investigation                                                                                                                                   |
| Classification | Three sensitivity tiers; higher-tier sites must connect live feeds to operations rooms via secure networks                                                                                 |
| Access         | MOI / State Security Presidency can access feeds; public disclosure barred without approval or court order                                                                                 |
| Penalties      | SAR 500 per non-compliant camera · SAR 1,000 per incorrect installation · up to SAR 5,000 for failure to retain recordings · up to SAR 20,000 for unlawful publication or equipment damage |

## Personal Data Protection Law (PDPL)

### CHALLENGE

Customer and payment data is collected across every branch.



### IMPACT

Legal basis and consent required; 72-hour SDAIA breach notification; mandatory Arabic/English privacy policies; cross-border transfer restrictions; fines up to SAR 5M, doubled on repeat; imprisonment up to two years for unauthorized disclosure of sensitive data.

PDPL's definition of personal data extends to any information that identifies an individual — including footage captured by surveillance cameras across your locations.

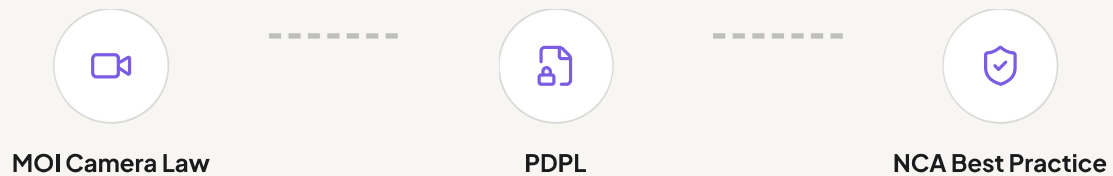
The background of the slide features several horizontal, wavy lines in a light purple color, creating a sense of movement and depth against the dark background.

# 04

## The Fragmentation Problem

## The Fragmentation Problem

Three different regimes govern a single F&B location. Each has its own obligations. None of them is coordinated by default — and multiplying that across ten, twenty, or fifty branches means the gaps multiply too.



Three regimes. Zero coordination by default.

A camera installed to satisfy the MOI decree still needs its footage handled under PDPL. A network segmented to best practice still needs to route camera feeds to an operations room the way the decree requires. Treated as three separate projects, compliance becomes three separate points of failure.

The background of the slide features several horizontal, wavy lines in a light purple color, creating a sense of movement and depth against the dark grey background.

# 05

## Self-Assessment Framework

# Self-Assessment Framework

Score your operation against these before an inspection does.

- 01 Are cameras installed and operational before each new location's license is granted or renewed?
- 02 Is footage retained unaltered and accessible for the period your classification tier requires?
- 03 Do you have a documented process to notify SDAIA within 72 hours of a data breach?
- 04 Are your privacy policies published in both Arabic and English at every branch?
- 05 Is your network segmented so a breach at one branch cannot reach another?
- 06 Do higher-tier sites have live camera feeds connected to an operations room over a secured network?
- 07 Do you know which of your locations, if any, fall under NCA ECC scope?
- 08 Is there a single owner accountable for cameras, network, and data protection together — or are they three vendors who don't talk to each other?

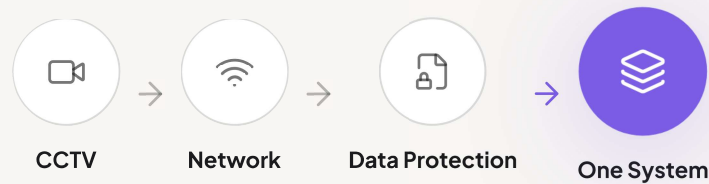
The background of the slide features several horizontal, wavy lines in a light purple color, creating a sense of motion and depth.

# 06

## The Case for Full-Stack Integration

## The Case for Full-Stack Integration

Physical security, network infrastructure, and data protection are being run as three separate problems by most multi-branch operators. They are one operational system.



This is where Magnaite works — full-stack systems integration across CCTV, networking, and the infrastructure data protection compliance runs on. Not a claim to cybersecurity-compliance breadth Magnaite doesn't own. The lane is physical and network infrastructure, built to hold up under the regulations that already apply to you.

## — CONCLUSION

# Conclusion

The regulatory reality facing Saudi F&B operators is more specific, and more actionable, than most compliance content suggests. NCA ECC isn't legally required for you. The MOI camera law and PDPL almost certainly do apply, in ways that touch every branch you operate — and choosing a partner who meets NCA's bar anyway is worth factoring in.

Acting on it means getting the parts that are already legally mandated right — installation, retention, notification, network segmentation — before growth outpaces the systems meant to protect it.

---

## References

1. Saudipedia — Law of the Use of Security Surveillance Cameras
2. SGC Consulting — NCA ECC Compliance Guide
3. GHS — NCA ECC-2:2024
4. CMS Law — One year on: Saudi PDPL
5. RH-ISAC / Verizon DBIR 2025 — Retail & Hospitality Industry Insights
6. IBM Cost of a Data Breach, Middle East 2025
7. Security MEA (Check Point regional threat data), February 2025
8. Infosecurity Magazine — KFC/McDonald's phishing campaign, October 2022



## About Magnaite

**Wired to Stay — 35 years of full-stack systems integration in Saudi Arabia.**

Magnaite has operated in Saudi Arabia since 1989, installing and maintaining the infrastructure multi-branch F&B operators run on: CCTV and AI analytics, networking, access control, and control rooms.

Our work sits across the systems this report covers — the cameras the MOI decree regulates, the networks that carry customer data under PDPL, and the infrastructure that has to hold up as you scale past one location.

**One integrator, one system, built to outlast the install.**

Learn more

[www.magnaite.com](http://www.magnaite.com)

[Request a Consultation](#)

[contact@magnaite.com](mailto:contact@magnaite.com) · Riyadh, Saudi Arabia

**Wired to Stay.**