Protecting Franchise Networks Against Cybercrimes

IBA/IFA Joint Conference | Workshop 3
Washington, D.C. | May 2026

IBA/IFA26
JOINT CONFERENCE

Moderator: Esmari Jonker

Speakers: Gustavo Alcocer | Dominic Mochrie

Contributor: Raynia Theodore

PROTECTING FRANCHISE NETWORKS AGAINST CYBERCRIMES

- Rapid digitalization of franchise systems has transformed modern franchise networks into highly interconnected and data-driven commercial ecosystems.
- Unique cybersecurity challenges
- Exponential increase in cyberattacks on franchise networks

RECENT ATTACKS ON FRANCHISE NETWORKS

YEAR	COMPANY	HOW THEY ATTACKED	IMPACT
2021	McDonalds	Hackers gained access to internal systems and extracted customer and employee data from multiple jurisdictions.	Exposure of employee and customer information across various countries.
2022	Uber Technologies Inc.	Attackers used stolen credentials and MFA fatigue techniques to gain privileged access to internal systems and administrative tools.	Broad compromise of internal systems; operational disruption.
2023	Yum! Brands (KFC, Pizza Hut, Taco Bell)	Ransomware actors disrupted IT infrastructure used by franchise operations.	+/- 300 restaurants in the United Kingdom temporarily closed; operational and financial losses.
2023	Caesars Entertainment	Threat actors manipulated IT help desk procedures and obtained access to customer loyalty databases, extortion demands were issued.	Exposure of customer loyalty data; reported ransom payment of +/- USD 15 million.
2023	MGM Resorts International	Attackers compromised IT systems through social engineering techniques, prolonged system outages.	Operational shutdowns for several days; estimated losses of approximately USD 100 million.

RECENT ATTACKS ON FRANCHISE NETWORKS

YEAR	COMPANY	HOW THEY ATTACKED	IMPACT
2024	Coppel	Attackers obtained access through compromised credentials, escalated privileges and deployed ransomware across servers and endpoints.	Operational disruption in retail and financial services; reputational harm and incident response costs.
2024	Subway	Attackers infiltrated company systems and threatened publication of stolen data.	Potential exposure of corporate and customer data; reputational and operational risk.
2024	Ultra Tune (Australia)	Attackers exfiltrated data including HR records, customer information and internal databases.	Exposure of passports, driver's licences, medical certificates and employee information; reputational and regulatory risk.
2025	Restaurant Brands International	Security researchers identified critical vulnerabilities in digital systems used by franchise operators, exposing systemic cybersecurity weaknesses.	Increased cyber risk across franchise platforms; remediation costs and reputational concerns.
2025	Wynn Resorts	Attackers compromised employee credentials and accessed human resources and payroll information.	Exposure of employee salary, HR and contact information; reputational and compliance implications.
2026	Starbucks	Attackers used fraudulent HR portals to harvest employee credentials and payroll information.	Compromise of employee login details and payroll-related data; increased phishing and fraud risk.

ARE FRANCHISE NETWORKS READY FOR A CYBERATTACK?

- **Legal risk -** statutory penalties, class actions, regulator scrutiny across multiple jurisdictions
- **Operational risk -** shut-down stores, broken POS systems, supply-chain failure
- **Reputational risk -** brand damage that affects the entire brand, the franchisor and every franchisee in the system, not only a single party

One incident may apply to all three risk aspects.

The legal framework must also cover all three.

THE FRANCHISE MODEL AND CYBERSECURITY VULNERABILITIES

- **Why franchise networks are uniquely vulnerable**
- A hybrid structure, one brand, many independent businesses, shared technology, multiplies the attack risk:
  - ➢Multiple entry points
  - ➢Shared systems
  - ➢Third-party dependencies
  - ➢The human factor

PATTERNS AND TYPOLOGIES OF CYBERATTACKS

- **Ransomware -** encrypts POS, ordering and back-office systems; stores cannot trade until restored
- **Data breaches -** payment cards, loyalty databases, employee records exfiltrated and sold or leaked
- **Phishing & social engineering -** fake e-mails, fake calls, deepfakes targeting franchisees and head office alike
- **Credential compromise -** stolen logins reused across systems; a franchisee's password becomes the network's password

The most successful attacks rely on human error, not technical sophistication

REGULATORY COMPLIANCE AND CROSS-BORDER CHALLENGES

One incident in a multi-country franchise system can trigger notification, disclosure and penalty exposure in many jurisdictions at once.

- **EU GDPR / UK GDPR** - 72-hour breach notification, fines up to 4% of global turnover
- **United States** - state-by-state (CCPA/CPRA, CDPA; sector specific laws (HIPAA, GLBA)
- **Canada (PIPEDA)** - mandatory breach reporting, record-keeping and further privacy law reforms proposed
- **Australia** - Privacy Act + NDB scheme; recent reforms increasing penalties and broadening coverage
- **Others** - Brazil (LGPD), Singapore (PDPA), South Africa (POPIA), Japan (APPI), UAE — increasingly aligned but not identical

OPERATIONAL STANDARDS & GOVERNANCE

- **NIST CSF** - Identify, Protect, Detect, Respond, Recover; flexible and widely understood by US regulators
- **ISO/IEC 27001** - certifiable ISMS standard; useful as a contractual benchmark for franchisees and vendors
- **CIS Controls** - prescriptive, prioritised, practical; strong baseline for store-level operations
- **SOC 2** - audit-grade evidence for shared head-office systems and customer-facing platforms

System-wide enforcement matters more than the framework.

LEGAL FRAMEWORKS AND CONTRACTUAL RISK ALLOCATION

The franchise agreement is a key cybersecurity document in the network.

- **Compliance obligations** - mandatory standards, training, software, evolving security policy
- **Data protection and confidentiality clauses** - protocols around collection, storage and handling
- **Audit rights** - right to inspect, test, and require remediation potentially at the franchisee's cost
- **Incident reporting** - defined timelines (24–72 hours), defined channels, defined information set
- **Indemnities & Insurance** - who pays for what, backed by required cyber cover with the franchisor as additional insured

Older agreements will not cover this – contractual amendments needed

KEY TAKEAWAYS

1. **Cyber is a board-level legal and business risk** — not just an IT line item.
2. **Franchise structure is the multiplier** — shared systems, third-party tools, hundreds or thousands of human entry points.
3. **The franchise agreement is the lever** — standards, audit, reporting, indemnities, insurance.
4. **Plan cross-border before the incident** — map regulators, language, deadlines and message lines in advance.
5. **Hold less data, watch your vendors** — minimization and supply-chain controls cut your exposure most.
6. **Insurance is necessary but not sufficient** — governance and culture add support.

THANK YOU