IBA/IFA 41st

ANNUAL JOINT CONFERENCE

*** * * * ***

The Future of Global Franchising: Innovations, Technologies, and New Markets

*** * * * ***

UNDER ATTACK: HOW TO PROTECT FRANCHISE NETWORKS AGAINST CYBERCRIMES

—

May 20, 2026

Washington, D.C. U.S.A.

Esmari Jonker
Smit & Van Wyk Inc
Pretoria, South Africa

Gustavo Alcocer
Olivares
Mexico City, Mexico

Dominic Mochrie
Osler, Hoskin & Harcourt LLP
Toronto, Canada

Raynia Theodore
MST Lawyers
Mount Waverley, Australia

TABLE OF CONTENTS

1. Introduction

The rapid digitalization of franchise systems has transformed modern franchise networks into highly interconnected and data-driven commercial ecosystems. While technological integration has enhanced operational efficiency, scalability, and customer engagement, it has simultaneously exposed franchise systems to increasingly sophisticated cybersecurity threats. Due to the hybrid structure of franchising, where independent franchisees operate within unified technological and brand infrastructures, cyber incidents within a single unit may rapidly escalate into network-wide operational, legal, and reputational crises. Recent international cyberattacks affecting major franchise brands, examples of which are set out in Exhibit A, demonstrate that franchise systems are uniquely vulnerable to systemic cyber risks.

This paper examines the legal and operational challenges associated with cybersecurity in franchise networks, with particular emphasis on the allocation of risk within decentralized yet interconnected systems operating across multiple jurisdictions. It analyzes common cyberattack patterns, contractual risk allocation, regulatory fragmentation, governance frameworks, incident response mechanisms, and third-party supply chain exposure. Drawing on comparative legal frameworks, industry standards, and practical case studies, the paper argues that effective cybersecurity in franchise systems requires an integrated approach combining legal governance, technological safeguards, operational oversight, and continuous risk management. A glossary of cybersecurity terms is attached as Exhibit B.

2. The Franchise Model and Cybersecurity Vulnerabilities

2.1 Hybrid Structure with Independent Ownership and a Unified Brand

Franchise systems are neither fully centralized entities nor fully independent businesses. Instead, they operate as hybrid organizational networks, combining centralized brand control with decentralized ownership and operations. This hybrid structure often introduces unique cybersecurity challenges.

Franchise networks consist of legally independent franchisees operating under a single brand identity. While this model supports rapid scaling and local entrepreneurship, it fragments accountability for cybersecurity. Franchisors typically define policies, procedures, and security standards, but the franchisees are primarily responsible for implementing and maintaining these systems.

There may be uncertainty over who is responsible for implementing and funding cybersecurity measures.[1] If the franchise agreement is not clear on accountability and division of responsibilities, franchisees may underinvest in security due to cost pressures, lack of expertise, or lack of prioritization. Franchisors may lack direct authority to enforce compliance across all locations. As a result, cybersecurity governance can become inconsistent, leaving weak points across the franchise system.

2.2 Shared Technological Infrastructure

Despite decentralized ownership, many franchise systems rely heavily on shared and interconnected technologies, such as point-of-sale (POS) systems, customer databases, loyalty and rewards programs, gift-card programs, payment processing systems, and cloud platforms. This type of system setup allows for franchise locations to act as a potential entry point for vulnerabilities and breaches can propagate laterally across systems. Additionally, the growing use of IoT devices and connected systems (e.g., kiosks, cameras, smart equipment) has significantly increased the number of entry points for cyberattacks. Given

[1] https://www.plantemoran.com/explore-our-thinking/insight/2022/08/cybersecurity-essentials-for-franchises-prevent-respond-comply

that the franchise model creates systemic cybersecurity risk, the security of the whole network often depends on its weakest participant.[2]

2.3 The Tension between Centralized Standards and Decentralized Execution

Franchisors generally enforce brand standards, customer experience requirements, and technology platforms (in many cases); however, implementation of such standards is usually decentralized with significant authority delegated to the franchisees, including operating day-to-day systems and security practices (patching, password management, and training). However, a challenge is that franchisees often have varying levels of technology sophistication, know-how, and may interpret security standards and policies differently.[3] Although this knowledge gap can be remedied with training, there may still be challenges in coordination, such as security requirements conflicting with operational priorities, like speed and cost.[4] There may be fragmentation in compliance driven by difficulty enforcing standards across locations and regulatory exposure varying by jurisdiction and franchisee practices. Thus, even with strong internal policies, execution failures at the local level can occur and undermine the system's security.

Some of the common vulnerabilities that can impact a franchise system which exacerbate the tension between centralized standards and decentralized execution are POS attacks, third-party risks, phishing attacks, and weak password practices.[5] When POS systems are compromised, they can become targets given their storage of sensitive customer information. Breaches in such systems can lead to significant damage for the brand overall. Third-party risks that exist may involve third-party vendors for IT services and payment or support services, which may not be within a franchisor or franchisee's direct control. Other widespread vulnerabilities include phishing attacks on franchise systems which can involve franchisee employees and targeted malware or ransomware that can spread across the network. In franchise systems, improper password management at the franchisee level despite standardized practices can lead to unauthorized access to critical systems and leave data exposed to breach risks. These risks are often exacerbated by the fact that franchise systems have large volumes of sometimes sensitive data and may have inconsistent security defenses based on how well franchisees execute franchisor policies surrounding cybersecurity.

The franchise model's structural characteristics, including hybrid governance, shared infrastructure, and decentralized execution, create a uniquely challenging cybersecurity environment. As a result, franchise systems require uniform cybersecurity standards and significant oversight over cybersecurity enforcement and compliance at the franchisee level.

3. Patterns and Typologies of Cyberattacks

Cyberattacks affecting franchise systems do not occur as isolated or purely opportunistic events. On the contrary, they exhibit identifiable, recurring, and strategically predictable patterns that reflect both the structural characteristics of franchise business models and the behavioral tendencies of attackers.

From a legal and operational standpoint, the relevance of identifying these patterns lies in the fact that foreseeability of risk directly affects the applicable standard of care. Where attack vectors are well-

[2]https://www.franchise.org/2016/05/protecting-your-brand-with-network-wide-security-measures

[3]https://www.pcicompliance.com/franchise-pci-compliance/

[4]https://www.pcicompliance.com/franchise-pci-compliance/

[5]https://thefranchisecto.com/cybersecurity-for-franchise-systems-where-you-re-most-exposed-a-franchise-specific-look-at-cybersecurity-gaps-and-how-to-tackle-them-with-shared-responsibility-models-between-franchisor-and-franchisee

documented and recurrent, failure to implement preventive measures may constitute not only operational negligence but also regulatory non-compliance and possibly result in contractual breach.

As reflected in the example cases that have been researched and, in some instances, worked on, franchise systems, by their very nature, are particularly susceptible to such patterned attacks due to their reliance on:

- Shared technological infrastructure;
- Centralized or interconnected databases;
- Multi-user access environments with varying levels of cybersecurity maturity; and
- Cross-border digital operations.

Cyber incidents within franchise environments frequently originate within the same interconnected ecosystem that enables operational efficiency, thereby transforming internal architecture into a primary risk vector.

3.1 Common Attack Vectors

Cyberattacks targeting franchise systems generally fall within four principal categories, each of which exploits specific structural or behavioral vulnerabilities. Cyberattacks affecting franchise systems tend to follow identifiable patterns:

(i) Ransomware Attacks: Encryption of Systems and Demands for Payment

Ransomware constitutes one of the most severe and disruptive forms of cyberattack in franchise environments. It involves the unauthorized infiltration of systems followed by:

- Encryption or blocking of critical operational data;
- Suspension of system functionality; and
- A demand for payment, typically in cryptocurrency, in exchange for system restoration.

The legal and operational impact of ransomware in franchise systems is particularly acute due to the interconnected nature of digital infrastructure. Unlike standalone enterprises, franchise networks often rely on shared platforms, while maintaining distinct third party independence, meaning that a single compromised endpoint may: propagate laterally across the network; disable multiple franchise units simultaneously; and interrupt core business functions such as payment processing, inventory management, and customer transactions.

This creates a multiplicative harm effect, transforming a localized intrusion into a system-wide operational crisis. Ransomware is especially critical because it may compromise several units at the same time and the business in general.

Ransomware incidents may trigger, among other, breach of contractual obligations; regulatory reporting duties under data protection laws in multiple jurisdictions; and liability exposure for failure to implement adequate safeguards.

(ii) Data Breaches: Unauthorized Access to Customer and Employee Data

Data breaches involve the unauthorized access, extraction, or exposure of sensitive information, including: personal identifiable information of customers and employees, financial and transactional data, trade secrets and proprietary business information.

In franchise systems, the risk profile of data breaches is significantly heightened due to: the existence of shared databases accessible by multiple franchisees; lack of uniform cybersecurity controls across different units; and the presence of numerous users with varying levels of standards, authorization and training.

This creates a scenario in which the entire network is vulnerable, particularly when access controls are not standardized. Legally, data breaches give rise to a complex matrix of obligations and liabilities, including: compliance with data protection regimes, notification obligations to affected individuals and authorities, and potential civil liability for damages resulting from unauthorized disclosure.

The interconnected architecture of franchise systems transforms what would otherwise be a contained breach into a network-wide exposure event, significantly increasing both legal and reputational risk.

(iii) Phishing and Social Engineering: Manipulation of Individuals to Gain Access Credentials

Phishing and social engineering attacks represent a category of threats that target human behavior rather than technological systems. These attacks typically involve: fraudulent communications designed to appear legitimate; requests for credentials, financial information, or system access; and inducement of users to click malicious links alter wire instructions or download harmful content.

In franchise systems, these attacks are particularly effective due to decentralized personnel structures, high turnover in certain operational roles, and inconsistent training across franchise units in the same footprint. The core characteristic of social engineering is that it leverages trust, urgency, and authority, rather than technical sophistication. Such attacks may involve phishing emails, impersonation of management or IT personnel, and manipulation of helpdesk staff to obtain unauthorized access, always taking advantage of remoteness of parties involved.

(iv) Credential Compromise: Exploitation of Weak Authentication Practices

Credential compromise attacks focus on obtaining valid login credentials through phishing schemes, password reuse exploitation, brute-force attacks, and credential stuffing.

Within franchise systems, the risk is amplified by: multiple access points across different units in different jurisdictions; lack of centralized identity and access management (IAM); and inconsistent enforcement of password policies and multi-factor authentication.

Once credentials are compromised, attackers may gain legitimate access pathways, allowing them to bypass traditional security controls and move laterally within the system. From a legal standpoint, failure to implement widely recognized authentication safeguards such as multi-factor authentication may be interpreted as a failure to meet industry-standard security practices.

3.2 The Role of Social Engineering

A central and empirically supported finding in cybersecurity is that the majority of successful attacks rely on human error rather than technical sophistication. Social engineering operates through psychological manipulation, exploiting factors such as trust in authority figures; sense of urgency; lack of awareness or training; and cognitive overload in operational environments.

The effectiveness of cyberattacks often lies not in their technical complexity but in their ability to deceive individuals, where mechanisms vary and change adding a layer of challenge in prevention and identification, as we have seen in unfortunate *phishing* - emails or messages designed to mimic legitimate communications, prompting users to disclose credentials or click malicious links. Other examples are *impersonation (pretexting)* where attackers pose as internal personnel (e.g., IT staff or management) to request access or password resets and *helpdesk fraud* - manipulation of support personnel to bypass authentication protocols and grant unauthorized access.

The critical implication is that even a technically robust system may be compromised through a single human error. This reality shifts cybersecurity from a purely technical domain into a governance and compliance issue, requiring continuous employee training, awareness programs, and procedural safeguards.

3.3 Systemic Risk Amplification

(i) Interconnectivity as a Risk Multiplier

Globalization has brought the need for interconnection and franchise systems function as integrated digital ecosystems, composed of central franchisor systems, franchisee operational platforms, third-party service providers, and shared databases and cloud infrastructure.

While this interconnectivity enhances efficiency, it simultaneously expands the attack surface or door and introduces systemic vulnerability. A cyber incident within such systems rarely remains isolated; rather, a single compromised node can escalate into a system-wide disruption.

(ii) The Concept of Network Amplification Risk

The phenomenon described above may be conceptualized as network amplification risk, defined as the exponential escalation of a cyber incident across interconnected systems due to shared infrastructure and access pathways. In practical terms, one compromised franchisee system may provide access to centralized databases, attackers may pivot across the network using legitimate credentials, and the impact may extend to hundreds of operational units.

(iii) Internal Origin of Cyber Incidents

A particularly relevant pattern is that cyber incidents do not necessarily originate externally. Instead, they often emerge from within the same digital ecosystem that connects the organization, including: compromised franchisee systems; third-party vendors; and internal user accounts.

This underscores the fact that the architecture of the business itself may constitute the primary source of risk, rather than external threats alone.

(iv) The Human Factor as the Weakest Link

Even in systems with advanced technical safeguards, human behavior remains the most vulnerable element. A single manipulated employee or vulnerable franchisee system can provide attackers access to centralized systems, impacting the entire network. This vulnerability is exacerbated in franchise systems due to large numbers of users, varying levels of cybersecurity awareness, and inconsistent implementation of security policies.

(v) Implications for Cybersecurity Governance

The systemic nature of cyber risk in franchise systems necessitates a holistic governance approach, integrating technological controls, organizational processes, and continuous human training. Effective cybersecurity cannot rely solely on IT defenses but must incorporate governance mechanisms that address human and organizational factors.

The analysis of patterns and typologies of cyberattacks reveals a fundamental principle: cyber risk in franchise systems is structural, predictable, and amplified by interconnectivity. Accordingly, the legal and operational responses must shift from reactive incident management to proactive risk identification, standardized security controls across the network, and continuous training and governance integration.

Failure to recognize and address these patterns does not merely expose franchise systems to cyber threats; it may also constitute a failure to meet the evolving legal standard of reasonable cybersecurity practices.

4. Cybersecurity as a Legal and Business Risk

4.1 Beyond IT: A Multidimensional Risk

For too long, cybersecurity has been treated as a technology problem - something to be delegated to the IT department and managed through software procurement and upgrades. Cybersecurity is not a technical issue with legal implications; it is a legal, operational, and reputational risk that has a technical aspect.

Franchise systems are, at their core, creatures of contract. The franchisor exercises control through brand standards and system manuals. When a cyber incident occurs, the question is not merely who was hacked, but who owed what obligations to whom, what did those obligations require, and were they met? These questions are fundamentally legal questions.

The multidimensional character of cyber risk in franchising can be understood across three overlapping key risks:

- ***Legal risk***: Exposure to regulatory investigation and enforcement, civil litigation (class actions) from affected customers, employees or franchisees, and liability for breach of contractual or statutory obligations. Data protection regimes have grown globally, and the regulatory complexity and costs of a breach have escalated dramatically. Fines, enforcement undertakings, class actions, and reputational damage are all live risks with real financial consequences in potentially multiple jurisdictions.

- ***Operational risk***: Cyber incidents can disrupt business continuity across an entire franchise network simultaneously. Ransomware that locks a franchisor's operational systems can prevent franchisees from processing transactions, accessing loyalty programs, or communicating with head office. The Yum! Brands attack in early 2023, which forced approximately 300 UK restaurants to close temporarily, illustrates how a single incident can cascade into network-wide operational failure.

- ***Reputational risk***: Perhaps the most underappreciated risk for franchisors is brand damage. A franchisor's brand is the foundational asset of a franchise network. Customer trust, once breached, is difficult and costly to rebuild. The reputational impact of a breach is rarely

contained to the franchisee who was directly compromised - it attaches to the brand itself, affecting every franchisee in the system.

Management advisers, including in-house counsel, must ensure that cybersecurity governance is embedded in the legal architecture of the franchise system and is not an add-on after an incident occurs.

4.2 Data Governance and Minimization - Prevention is Better than Cure

Effective risk management requires identifying critical data assets, limiting data collection to necessary information, and implementing classification and protection protocols. Data minimization reduces exposure and aligns with global privacy principles. **Put simply: you cannot lose data you do not hold.**

Franchise networks, by their nature, accumulate vast quantities of data. Customer transaction records, loyalty program databases, employee and franchisee personal information, payment card data, supplier contracts, franchisee financial records, and proprietary operational information all flow through franchise systems on a daily basis. This data is of significant value - but it also creates significant exposure. A franchisor who collects and retains more data than necessary is not merely inefficient; they are creating unquantified exposure and liability.

Implementing a disciplined approach to data governance requires franchisors to ask and honestly answer three foundational questions about every category of data they collect or control:

- What information is actually needed to operate the franchise system effectively?
- What is it needed for, and does that purpose justify the collection and retention of that data?
- Why is it being held, and for how long - and is there a clear, legally defensible basis for doing so?

In practical terms, a data governance program for a franchise network should include the following elements:

- **Data asset inventory**: identifying and mapping all categories of data collected, processed, or stored by the franchisor and across the network, including data held by franchisees and third-party vendors. The assessment process should identify critical data, systems, and processes (customer data, financials, IP, operational platforms); classify data by sensitivity and regulatory impact, including shared or jointly held data (e.g., franchise networks, partners, vendors); and apply stronger controls (encryption, access restrictions, monitoring) to high-value assets.

- **Data classification**: categorizing data by sensitivity and risk profile - for example, distinguishing between publicly available information, internal operational data, personal data, sensitive personal data (including health and financial information), and trade secrets or confidential business information.

- **Access controls and segmentation**: ensuring that access to high-value or sensitive data is restricted to those who genuinely need it, with appropriate authentication requirements (including multi-factor authentication) and logging of access events.

- **Retention and destruction policies**: establishing clear timelines for data retention aligned with legal requirements, business needs, and privacy principles, together with enforceable protocols for the secure destruction of data that is no longer required. This is particularly important in the franchise context, where franchisee agreements expire or terminate and the ongoing handling of data must be contractually addressed.

- **Shared and jointly held data**: franchise networks frequently involve data that is shared between the franchisor, franchisees, and third-party vendors. The legal characterization of these relationships - who is a data controller, who is a data processor, and what obligations attach to each - varies across jurisdictions and must be carefully mapped and documented.

Strong data governance is not just a risk mitigation tool; it is a compliance necessity. Regulators in jurisdictions including the EU, UK, and Australia have made clear that organizations that cannot demonstrate effective governance of the data they hold will face heightened scrutiny in the event of a breach. A franchisor will be in a materially stronger position if it can show that it collected only what it needed, classified it appropriately, controlled access carefully, and deleted it when no longer required when engaging with regulators, managing litigation, and preserving brand trust.

For franchise lawyers, the practical takeaway is this: data governance and minimization should be treated as a front-end legal exercise, not a compliance afterthought. The time to build those frameworks is before the breach, not after. The key takeaway for franchise networks is that they should not collect and hold more than what is needed. Franchisors can minimize potential exposure by limiting critical information under their control and having destruction-of-data policies and protocols, subject to law.

5. Legal Frameworks and Contractual Risk Allocation

5.1 Contracts

Franchise cybersecurity risk is governed largely through contracts. Of all the contracts franchisors and franchisees are required to enter into to operate in the franchise space, franchise agreements are the primary mechanism for allocating cyber risk across independent operators. Franchisors use such contracts to enforce system standards and operational and technological consistency across franchisees in the system. Given the shared but fragmented responsibility within franchise systems, such contractual clarity is important to manage risk appropriately.

Some of the requirements imposed on franchisors and franchisees are contractual in nature, whereas others are driven by legislation.[6] In Canada, for example, data collection, use, and disclosure requirements for all organizations, including franchisors and franchisees, are imposed by the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("PIPEDA"), or provincially similar legislation. Additionally, on the contractual side, similar and additional obligations are typically imposed on franchisees pursuant to the confidentiality and data protection provisions of the applicable franchise agreement.

Some of the key provisions of note for franchisors regarding cybersecurity within franchise agreements include cybersecurity compliance obligations, data protection and confidentiality clauses, audit and inspection rights, incident reporting requirements, and indemnities and liability allocation.[7]

(i) Cybersecurity Compliance & Standards

Cybersecurity compliance clauses impose affirmative, ongoing duties on franchisees to meet defined security standards. Such provisions are usually not generic "reasonable efforts" clauses and are increasingly technical and prescriptive. Typical elements may include compliance with prescribed standards (e.g., ISO), use of approved franchisor systems (e.g., POS and cloud tools), required safeguards (e.g., encryption, patching, access controls), employee training and supervision, and access management

[6]https://cfa.ca/franchisecanada/q-what-do-franchisees-need-to-know-about-cybersecurity-and-data-protection-risk-mitigation

[7]https://cfa.ca/franchisecanada/q-what-do-franchisees-need-to-know-about-cybersecurity-and-data-protection-risk-mitigation

requirements and security roles within systems for designated employees. Specific procedural requirements may also be required such as two-factor authentication, complex password policies, data protection agreements, and cybersecurity insurance.[8] Franchise agreements increasingly incorporate information security requirements into vendor selection and the design of the franchise system.

(ii) Artificial Intelligence

The groundswell of artificial intelligence has created some additional complexity, as it has not historically been contemplated in the franchise agreement, though the topic could be covered by general technology provisions. Including specific provisions relating to the use of AI in the franchise agreement for new franchisees or renewing franchisees is certainly a viable option, but that doesn't address those franchisees on legacy and long-term agreements.

(iii) Data Protection & Stewardship

When considering data protection and confidentiality clauses in the context of cybersecurity, they serve multiple purposes. Such provisions define what constitutes "confidential information," how personal data may be handled, and who owns and controls different types of data. They will often include restrictions on data use and disclosure, and data ownership provisions, often involving certain types of data ownership retained by the franchisor. Historically, franchise agreements provided that the franchisor owned all consumer information. However, more recently there is a trend that franchisors do not want to undertake the stewardship obligations of personal information collected by their franchisees. Further to this, there may be return or destruction obligations on termination set out in the franchise agreement. While franchisors often "own" the data, the franchisee collects and processes data, which can create joint liability exposure in the event of breaches. As a result of the complexity involved in breaches, contracting often involves intricate data governance frameworks.

(iv) Audit and Inspection Rights

Audit and inspection right clauses give franchisors the right to inspect franchisee systems, verify compliance with contractual obligations, and detect financial and operational discrepancies.[9] It is important to ensure that there is an appropriate balance between franchisor's rights and franchisees' compliance obligations in audit clauses to protect the franchisor's interests without going beyond what is reasonably necessary to impose on a franchisee.

(v) Incident Reporting & Remediation

A franchise agreement must stipulate an affirmative obligation for franchisees to provide immediate notification upon the discovery of a suspected security compromise. Beyond mere reporting, these provisions serve as a critical mechanism for loss allocation; they should explicitly assign the financial burden of forensic investigations, consumer notification, and technical remediation to the franchisee, provided the breach originated within their delegated operational environment. By contractually localizing this fiscal responsibility, the franchisor mitigates the risk of systemic financial "leakage" while incentivising franchisees to maintain rigorous local security protocols.

(vi) Indemnification and Insurance

[8]https://cfa.ca/franchisecanada/q-what-do-franchisees-need-to-know-about-cybersecurity-and-data-protection-risk-mitigation

[9]https://www.swaab.com.au/publication/5-clauses-to-look-out-for-in-your-franchise-agreement-they-might-be-unfair

Robust indemnification provisions are paramount to insulating the franchisor from third-party liabilities, statutory penalties, and consequential damages arising from a franchisee's cybersecurity failure. To ensure these contractual protections remain solvent and enforceable, the agreement should mandate that franchisees maintain comprehensive cyber insurance policies. These policies act as a vital fiscal backstop, transforming the franchisee's abstract duty to indemnify into a tangible ability to satisfy significant claims, thereby preserving the financial integrity of the broader franchise system against catastrophic localized events.

(vii) Operational Delegation and Standardisation

A franchise agreement must meticulously delineate the distinction between the franchisor's "normative control" - the authority to mandate system-wide technical standards - and the franchisee's responsibility for "operational execution." By formalising this separation, the franchisor preserves its ability to implement essential security updates across the network while effectively insulating itself from the day-to-day management risks that might otherwise precipitate "joint-employer" status or vicarious liability claims. This structural decoupling ensures that the franchisor's oversight remains focused on brand integrity and network resilience rather than the minutiae of localized technical administration.

(viii) Strategic Allocation of Financial Burden

Beyond bilateral indemnification, the franchise agreement should address the "shared-cost" reality of network-wide vulnerabilities. Modern clauses must precisely calibrate the apportionment of costs associated with emergency system-wide patches, forensic audits of shared infrastructure, and hardware upgrades necessitated by evolving threats. By explicitly defining the financial threshold where franchisee responsibility ends and collective or franchisor-led investment begins, the agreement ensures that the economic burden of securing hundreds of independent nodes does not result in systemic insolvency or a failure to implement mission-critical security interventions.

5.2 Static Compared to Dynamic Contracting Standards

In addition to standard clauses, there may be drafting issues that franchisors and franchisees should stay aware of, such as static compared to dynamic standards that are imposed on franchisees. Agreements increasingly incorporate standards that may be "updated from time to time" to avoid obsolescence and allow for flexibility in the change of systems and processes. At times, security policies may be only incorporated by reference, since this allows franchisors to easily update them more frequently than contracts may be updated. On the other hand, technology usage requirements may be more rigid contractual requirements to reduce system risk by requiring only franchisor-approved systems to reduce system vulnerabilities.

6. Regulatory Compliance and Cross-Border Challenges

6.1 Fragmented Global Regulatory Landscape

Franchise systems operating internationally must navigate diverse legal regimes governing data protection, breach notification, and cybersecurity standards. One of the most challenging dimensions of cybersecurity governance for international franchise systems is the sheer complexity of the regulatory environment in which they operate. There is no single global standard for data protection, no uniform breach notification regime, and no harmonized set of cybersecurity obligations. Instead, franchise systems operating across multiple jurisdictions must navigate a patchwork of divergent, and sometimes conflicting, legal requirements.

The most significant data protection frameworks currently in force include:

- ***European Union***: The General Data Protection Regulation (GDPR) applies to any organization processing the personal data of EU residents, regardless of where the organization is established. It imposes obligations regarding lawful processing, data subject rights, privacy by design, data protection impact assessments, and mandatory breach notification to supervisory authorities within 72 hours of discovering a breach. Non-compliance can attract fines of up to €20 million or 4% of global annual turnover, whichever is higher.

- ***United Kingdom***: Following Brexit, the UK GDPR and the Data Protection Act 2018 create a regime broadly equivalent to the EU GDPR, though divergence is anticipated over time. UK businesses that also operate in the EU must navigate dual compliance obligations.

- ***United States***: There is no single federal privacy law in the US. Franchise systems must instead navigate a complex matrix of state-level legislation, including the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), Virginia's Consumer Data Protection Act (CDPA), Colorado, Connecticut, Texas, Florida, and a growing number of additional states with enacted or pending privacy legislation. Sector-specific federal laws, including HIPAA (health), GLBA (financial services), and COPPA (children's online data), may also apply depending on the nature of the franchise system.

- ***Canada***: The Personal Information Protection and Electronic Documents Act (PIPEDA) applies to private sector organizations handling personal information in commercial activities, with mandatory breach notification requirements introduced in 2018. Significant reform is underway through Bill C-27, which, if enacted, will substantially update the Canadian framework.

- ***Australia***: The Privacy Act 1988 (Cth), as administered by the Office of the Australian Information Commissioner (OAIC), governs the handling of personal information by organizations with an annual turnover exceeding AUD 3 million. Mandatory data breach notification requirements have applied since 2018 under the Notifiable Data Breaches (NDB) scheme. Significant reforms to the Privacy Act — many of which are currently being legislated — will substantially strengthen obligations, including expanded definition of personal information, stronger consent requirements, a direct right of action for individuals, and increased penalties.

- ***Brazil***: The Lei Geral de Proteção de Dados (LGPD), which came into full force in 2021, broadly mirrors the GDPR in structure and creates comprehensive obligations for organizations processing the personal data of Brazilian residents.

- ***Other jurisdictions***: Comprehensive data protection legislation now exists in Singapore (PDPA), Japan (APPI), South Korea (PIPA), South Africa (POPIA), India (DPDP Act 2023), and an expanding range of other countries. Many Gulf Cooperation Council states have enacted or are in the process of enacting data protection legislation.

For franchise systems with international operations, compliance cannot be managed on a jurisdiction-by-jurisdiction basis in isolation. A data breach affecting a centralized franchise database will simultaneously trigger notification obligations in multiple jurisdictions, each with potentially different timeframes, thresholds, content requirements, and regulatory recipients. Managing that complexity requires thorough preparation.

6.2 Cross-Border Incident Management

Cyber incidents frequently involve multiple jurisdictions, requiring coordinated regulatory reporting, consistent communication strategies, and centralized incident response frameworks. When a cyber incident occurs in a franchise network that spans multiple countries, the franchisor faces an immediate and acute challenge - how to manage a coordinated, legally compliant response across jurisdictions that may have fundamentally different legal requirements and significantly different notification timelines.

Some key points for effective cross-border incident management are:

- ***Centralized coordination***: The franchisor must assume responsibility for managing the incident response centrally. Individual franchisees should not be left to manage regulatory notifications or customer communications independently. Inconsistent or fragmented responses create regulatory risk, amplify brand damage, and increase legal exposure. All communications, both internal and external, should be coordinated through a designated incident response team that includes legal counsel.

- ***Consistent messaging***: In a high-profile cyber incident affecting a recognized brand, including a franchise brand, media and regulatory attention is rapid and intense. The same factual account must be communicated consistently across all jurisdictions. Contradictory statements, whether from the franchisor, an individual franchisee, or a third-party vendor, will be identified and used against the organization. Legal privilege should be carefully maintained over all internal communications from the outset.

- ***Regulatory notification mapping***: Before an incident occurs, the franchisor's legal team should have mapped the notification obligations applicable in each jurisdiction of operation. This map should include the identity of the relevant authority, the notification timeframe (which ranges from 24 hours in some jurisdictions to 72 hours under the GDPR to "without unreasonable delay" in others), the threshold for notification (whether the breach must meet a harm-based test or is presumptively notifiable), and the required content of notifications.

- ***Individual notification obligations***: Separate from regulator notification, many jurisdictions require affected individuals to be notified where a breach is likely to result in a high risk to their rights and freedoms (GDPR), a real risk of serious harm (Australia's NDB scheme), or a significant risk of harm (various US state laws). The threshold, timing, and method of individual notification varies, and the content of notifications must be carefully calibrated to avoid creating admissions against interest in subsequent litigation.

- ***Data transfer implications***: In some circumstances, the forensic investigation of a cyber incident will require the transfer of personal data across borders for analysis. This may itself trigger data transfer compliance obligations under the GDPR and other frameworks, adding a further layer of complexity to what is already a high-pressure response environment.

The practical implication for lawyers is clear: franchisors who operate cross-borders must have a cross-border incident response, which requires a pre-existing framework, pre-approved communication templates, identified legal counsel in each key jurisdiction, and a documented escalation protocol. Organizations that have invested in this preparation will manage incidents better, both legally and operationally, than those who have not, and potentially minimize brand damage.

6.3 Asymmetry in Legal Obligations

In some jurisdictions, franchisors may be subject to stricter data protection laws than franchisees, creating compliance gaps and enforcement challenges. One of the most structurally challenging issues in cybersecurity compliance for franchise networks is the asymmetry that often exists between the legal obligations imposed on franchisors and those applicable to franchisees.

The Australian experience provides a useful illustration of this challenge. Under the Privacy Act, the default position is that small businesses - being businesses with an annual turnover of AUD $3 million or less - are exempt from the Act's requirements unless they fall into a category of small business that is caught by the Privacy Act, e.g., private sector health service providers which provide health services (e.g., fitness centers). The rationale for the exemption is the perceived regulatory burden on small operators. However, the practical consequence in a franchise network is that the franchisor is fully bound by the Privacy Act, including the Notifiable Data Breaches scheme, while most of its franchisees are not. The asymmetry between franchisors and (often exempt) franchisees creates some very real structural and risk issues across a franchise network because franchisees are not, and do not consider themselves, bound by privacy laws.

This creates a series of real and immediate issues for the franchise network:

- Franchisees may collect, handle, and retain customer personal data without any of the compliance obligations that bind the franchisor, including the obligation to implement reasonable security measures.

- A data breach originating at a franchisee level, which, as discussed in earlier sections of this paper, is a significant and realistic risk, may not trigger any direct compliance obligation on the franchisee, even though the franchisor may be required to notify the regulator and affected individuals because it owns the data.
- Franchisees who do not consider themselves bound by privacy law have little or no incentive to invest in the security infrastructure, training, and governance processes that would protect the franchise network as a whole.

- The franchisor's ability to manage a coherent, system-wide response to a breach is hampered when franchisees do not have parallel legal obligations to cooperate, report, and implement remediation measures.

In the EU and UK, while the GDPR applies regardless of business size, the practical compliance appetite and capability of franchisees may be significantly less than that of the franchisor.

The solution to this asymmetry lies primarily in the franchise agreement. Where the law does not impose equivalent obligations on franchisees, the franchisor must achieve compliance through contractual means. This is addressed in more detail in Section 5 of this paper, but the key point is that franchise agreements must be used to contractually impose on franchisees the data protection and cybersecurity obligations that the franchisor needs to meet its own legal requirements and to manage system-wide risk. This includes obligations to implement minimum security standards, to report suspected breaches to the franchisor immediately, to cooperate with incident response processes, and to maintain appropriate technical and organizational measures.

Contractual compliance mechanisms are only as effective as their enforcement. Franchisors must be willing and able to audit franchisee compliance, and franchise agreements must contain effective

remedies, including the right to require immediate remediation and, in serious cases, to terminate the franchise in the event of material non-compliance with cybersecurity obligations.

When an incident occurs, the franchisor should:

- Centrally manage the incident. Messaging must be consistent across jurisdictions.
- Notify the regulator and individuals - notification will be required in most jurisdictions; timeframes may vary.
- Apply a cross-border response framework that takes into account all countries the franchise network operates in.

7. Operational and Governance Strategies

Cybersecurity within franchise systems must be approached not merely as a technical safeguard, but as a comprehensive governance function integrating legal compliance, operational control, and risk management. Given the inherently interconnected and decentralized structure of franchise networks, cybersecurity risks are both distributed and systemic, requiring coordinated strategies that transcend individual entities.

Franchise systems operate as integrated digital ecosystems, in which franchisors, franchisees, and third-party providers share technological infrastructure, data repositories, and operational platforms. While this integration enhances efficiency and scalability, it simultaneously expands the attack surface and creates system-wide exposure to cyber risk. Consequently, cybersecurity governance must be implemented not at the level of isolated entities, but across the entire network as a unified risk environment.

From a legal perspective, this entails establishing uniform cybersecurity standards across all franchisees, ensuring compliance with cross-border regulatory frameworks, and embedding cybersecurity obligations within contractual and operational structures.

7.1 Adoption of International Standards

A central pillar of effective cybersecurity governance is the adoption of internationally recognized frameworks, which provide structured methodologies for identifying, managing, and mitigating cyber risks. These frameworks serve as benchmarks for the standard of care, increasingly used by regulators and courts to assess whether an organization has implemented "reasonable security measures."

(i) NIST Cybersecurity Framework (CSF): Risk-Based Governance Model

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is widely regarded as the leading global reference for cybersecurity risk management. It is structured around five core functions: Identify, Protect, Detect, Respond, and Recover.

This framework emphasizes a risk-based and adaptive approach, enabling organizations to align cybersecurity measures with business objectives and threat environments. In franchise systems, the NIST framework is particularly valuable because it supports enterprise-wide risk management across multiple entities, facilitates standardization of controls across franchisees, and provides a scalable model adaptable to both large franchisors and smaller franchise units. However, implementation requires significant financial investment, organizational alignment, and continuous evaluation and updating of controls.

(ii) ISO/IEC 27001: Information Security Management Systems (ISMS)

The International Organization for Standardization ISO/IEC 27001 standard establishes a formal Information Security Management System (ISMS). Its core function is to ensure that organizations systematically identify risks, implement appropriate security controls, and maintain continuous monitoring and improvement.

For franchise systems, ISO 27001 offers a certifiable framework, enhancing credibility and trust; a structured method for integrating technical, organizational, and human controls; and a basis for cross-border harmonization of cybersecurity practices. Nevertheless, certification entails development of internal policies and procedures, ongoing audits and compliance verification, and continuous training of personnel.

(iii) CIS Critical Security Controls: Operational Prioritization

The Center for Internet Security CIS Controls provide a prioritized set of technical and operational safeguards designed to mitigate the most common cyber threats. These controls focus on access management, vulnerability management, data protection, and incident response. Their relevance in franchise systems lies in their practical applicability, particularly for standardizing baseline security measures across franchise units, addressing common vulnerabilities such as credential compromise and misconfigurations, and providing actionable guidance that can be implemented regardless of organizational size.

(iv) SOC 2 Framework: Trust and Assurance in Data Handling

The American Institute of Certified Public Accountants SOC 2 framework evaluates organizational controls based on five trust service criteria: Security, Availability, Confidentiality, Processing Integrity, and Privacy. SOC 2 is particularly relevant in franchise systems that process customer data, rely on cloud-based services, or operate in sectors requiring high levels of trust (e.g., financial services, retail). It provides assurance to stakeholders, evidence of compliance with recognized standards, and a mechanism for evaluating third-party service providers.

7.2 Implementation Challenges in Franchise Systems

Although frameworks such as NIST, ISO/IEC 27001, CIS Controls, and SOC 2 provide structured approaches to cybersecurity, their implementation in franchise systems presents three core challenges: cost allocation, human risk, and enforcement.

First, cybersecurity requires significant investment in technology, personnel, and audits. In franchise systems, however, the franchisor typically defines the standards while franchisees bear the operational costs. Absent clear contractual allocation, this results in uneven compliance and increased systemic vulnerability.

Second, the primary risk is human. Effective implementation requires continuous training and awareness programs, yet franchise systems face inconsistent training standards, high employee turnover, and limited control by the franchisor over personnel. A single compromised user may expose the entire network.

Third, cybersecurity requires ongoing monitoring and enforcement. Without centralized oversight, standardized reporting, and enforceable audit mechanisms, compliance becomes fragmented, and the system operates at the level of its weakest participant.

7.3 Cross-Border Governance and Regulatory Fragmentation

Cybersecurity governance is further complicated by regulatory fragmentation across jurisdictions. In the United States, the National Institute of Standards and Technology (NIST) provides a centralized and widely accepted framework. By contrast, in Mexico, responsibilities are distributed among multiple authorities. This lack of uniformity creates inconsistent regulatory expectations, increases compliance complexity, and complicates the harmonization of cybersecurity policies in cross-border franchise systems.

7.4 Governance Integration

Effective cybersecurity in franchise systems requires integration of three elements: technology, processes, and legal enforcement. Technologically, baseline controls such as encryption and access management must be standardized across all units. Operationally, organizations must implement risk management protocols, incident response plans, and regular audits. Legally, franchisors must impose binding cybersecurity obligations through franchise agreements, including audit rights and enforcement mechanisms.

Given the interconnected nature of franchise systems, cybersecurity must be treated as a collective responsibility. A single vulnerable unit may compromise the entire network. The adoption of cybersecurity standards in franchise systems is essential, but effectiveness depends on governance. Clear allocation of responsibilities, consistent training, and centralized enforcement are necessary to ensure uniform risk management. In interconnected systems, security ultimately depends on the weakest link.

7.5 Technology Control and Platform Governance

Franchise agreements increasingly include provisions granting franchisors control over technological infrastructure, including: mandatory use of approved IT systems; control over websites, applications, and digital content; centralized approval of vendors and service providers; and implementation of franchisor-designated platforms.

These clauses reinforce standardization across the network, which is essential for both operational efficiency and cybersecurity. A recurring issue is that contracts often require the use of specific systems but do not always impose explicit minimum cybersecurity standards. This creates a regulatory and contractual gap, where technological control exists without fully articulated security obligations.

7.6 Cyber Insurance and Risk Transfer Mechanism

Another emerging contractual trend, as in other transactions, is the inclusion of insurance requirements, including business interruption coverage; professional liability and directors and officers insurance; civil liability coverage; and optional cyber insurance for first-party and third-party losses.

Cyber insurance, in particular, functions as a risk mitigation tool, allowing franchise systems to transfer part of the financial exposure associated with cyber incidents. However, as seen in the sample clauses, cyber insurance is often optional rather than mandatory and left to the discretion of the franchisee. This approach may weaken the overall risk management strategy, as inconsistent insurance coverage across the network can lead to unequal protection and increased systemic exposure.

7.7 Key Legal Gaps and Practical Implications

Despite the increasing sophistication of cybersecurity clauses in franchise agreements, significant gaps remain. These include the absence of uniform security standards across franchisees, an over-reliance

on broadly drafted obligations lacking technical specificity, insufficient regulation of incident response procedures, and inconsistent allocation of cost and liabilities.

From a legal perspective, these deficiencies may expose franchise systems to regulatory sanctions for non-compliance with data protection laws, civil liability for failure to implement reasonable security measures, and reputational harm arising from network-wide breaches.

The evolution of cybersecurity provisions reflects a broader shift toward the contractualization of digital risk. However, effective risk management requires more than formal compliance. It demands clear allocation of responsibilities, enforceable security standards, and alignment between contractual obligations and their technical implementation. Absent such alignment, contractual provisions risk remaining formally compliant but operationally ineffective, leaving franchise systems exposed to systemic cyber risk.

8. Third-Party Risk and Supply Chain Exposure

Franchise systems rely heavily on external vendors, necessitating comprehensive due diligence, clear contractual obligations, and continuous monitoring of vendor performance. Third-party breaches can have system-wide consequences, reinforcing the need for integrated risk management.

The cybersecurity risk profile of a franchise network is not assessed by reference to the franchisor and franchisee alone. Franchise systems are embedded in extended supply chains and rely on third-party vendors-technology providers, payment processors, point-of-sale system operators, cloud storage providers, marketing platforms, loyalty program administrators, and many others. Each of these vendors will have some degree of access to network systems, data, or both. Each of those relationships is a potential vulnerability.

The 2013 Target data breach, though not a franchise case, remains a well-recognized illustration of the risks associated with third-party supply chains. Attackers gained access to Target's network through credentials stolen from an HVAC subcontractor, ultimately compromising the payment card data of approximately 40 million customers, including credit and debit card numbers, as well as the personal data of 70 million customers.

The lesson is not that franchise systems must avoid using such vendors - they cannot operate without such vendors. The lesson is that vendor relationships must be treated as security relationships, not merely commercial ones.

In the franchise context, third-party risk is amplified by scale. A franchise system with hundreds or thousands of locations may rely on a single point-of-sale software provider, a single payment processing platform, or a single cloud-hosted operational management system. If that vendor is compromised, the breach is immediately system-wide. The 2025 Restaurant Brands International vulnerability disclosure identified serious flaws in the digital platforms used across the KFC, Burger King, Popeyes, and Tim Hortons networks and illustrates precisely the risks for franchise networks.

Effective third-party risk management in a franchise network requires a structured approach to third-party vendor risk management, including:

- ***Vendor identification and registration***: Maintain a comprehensive and current register of all third parties with access to the franchise network's systems or data. This should capture the nature of the access, the categories of data involved, the jurisdictions in which the vendor operates, and the applicable contractual and regulatory framework.

- ***Pre-engagement due diligence***: Before engaging a vendor, conduct security-focused due diligence proportionate to the risk profile of the engagement. For high-risk vendors - those with access to sensitive personal data, payment systems, or core operational infrastructure - this should include review of the vendor's security certifications, such as ISO/IEC 27001 or SOC 2, penetration testing records, incident history, and data handling practices.

- ***Contractual protections***: Every vendor contract should contain clear and enforceable cybersecurity obligations. These should include minimum security standards, requirements to notify the franchisor of any actual or suspected security incident affecting the franchisor's data within a specified timeframe (typically 24–48 hours), obligations to cooperate with forensic investigation and incident response, rights of audit and inspection, data handling and deletion requirements, and liability and indemnification provisions. In jurisdictions covered by the GDPR or equivalent frameworks, appropriate data processing agreements must be in place.

- ***Clear allocation of responsibilities***: A common vulnerability in complex vendor relationships is ambiguity about who is responsible for what. Who is responsible for applying security patches? Who monitors for anomalous activity? Who holds incident response responsibility if a breach is identified? These questions should be answered in the contract and operationalized in documented governance arrangements and should not be left to be resolved once an incident has occurred.

- ***Ongoing monitoring and assessment***: Vendor due diligence is not a one-time exercise at the onboarding phase. Vendor security postures change, new vulnerabilities emerge, vendor personnel change, and commercial pressures may lead vendors to cut corners on security investment. Franchisors should implement a program of ongoing vendor monitoring (at least annually) that includes periodic reassessment, review of security certifications upon renewal, and continuous monitoring of threat intelligence relevant to key vendors.

- ***Subcontractor visibility***: Many vendors themselves rely on subcontractors, creating a further tier of supply chain risk. Franchise agreements and vendor contracts should require disclosure and potentially approval of material subcontractors with access to the network's systems or data and should ensure that subcontractors are subject to equivalent security obligations.

For lawyers advising on vendor management, the practical challenge is often one of scale. A franchisor with a large network may have hundreds of vendor relationships, and it is neither practical nor cost-effective to apply the same level of due diligence to every one of them. Risk assessment is essential. Franchise networks should identify the vendors who represent the greatest potential exposure and apply enhanced due diligence and contractual protections to those relationships.

The key point to note is that third-party risk cannot be managed by contract alone. Contracts set the legal framework and allocate liability, but they do not prevent breaches. A vendor who does not invest in security will remain a risk regardless of the contractual obligations imposed on them. Franchisors must act when their monitoring identifies issues and require remediation of deficiencies identified, escalation where remediation is inadequate, and in serious cases termination of vendor relationships that represent unacceptable ongoing risk to the franchise network.

9. Training and Culture

A strong cybersecurity culture requires continuous behavioral reinforcement, not one-time compliance training. In franchise systems, where operational consistency is critical but technical sophistication varies across franchisees, building a cybersecurity-aware culture is especially important.

9.1 Operationalizing Cybersecurity Awareness in Franchise Environments

Ongoing cybersecurity training is an important aspect of maintaining awareness. Training programs focused on educating employees to recognize threats such as phishing, social engineering, and data handling risks are valuable, particularly when such training includes reinforcement mechanisms such as microlearning and periodic refreshers. For franchisees, training should not be annual or generalized; it should be embedded into operations with specific and real-life examples relating to franchise system scenarios involving POS systems, vendor payments, and handling customer data. For example, simulated phishing attacks are often used to test employee behavior and reinforce training by exposing employees to plausible attack scenarios and measuring their reactions.[10]

9.2 Making the Business Case for Cybersecurity in Franchise Systems

A challenge that can manifest in franchise systems is that cybersecurity measures, especially training and simulations, are often viewed as cost centers imposed on franchisees, who are primarily focused on profitability. This can create a tension between compliance and operational priorities. Research on SMEs indicates that smaller businesses are more vulnerable to cyberattacks due to limited resources and expertise. This makes investment in awareness programs more critical.[11] To promote adoption, franchisors should frame cybersecurity training by emphasizing financial and operational terms, not just compliance. They should focus on real-world loss scenarios, examples of the consequences of operational disruption, and the implications of system risk.

10. Incident Response and Crisis Management

10.1 Immediate Response Measures

Effective incident response depends on speed, coordination, and access to expertise. It is usually the first few hours following a cybersecurity incident that are critical to limiting legal, financial, and operational exposure. An effective immediate response generally requires a multi-disciplinary approach which begins with involving legal counsel, coordinating all relevant business units, and quickly gathering information about the incident. For example, a prompt forensic investigation will be valuable to determine the scope and root cause of the incident, systems and data affected, and whether the threat is ongoing. Such investigations will likely include structured evidence collection and analysis to support both remediation and potential future legal or regulatory proceedings.[12] To coordinate business units appropriately, franchisors and franchisees should have clearly defined roles and cross-functional coordination during incident response.[13]

10.2 Communication and Disclosure

Managing communications during and after a cybersecurity incident is both a legal requirement and necessary from a brand equity and reputation perspective. Organizations are subject to breach notification requirements in many jurisdictions. For example, in Canada, PIPEDA requires that organizations report breaches posing a “real risk of significant harm” to the Privacy Commissioner and

[10]https://www.techtarget.com/searchsecurity/feature/Do-phishing-simulations-work-Sometimes

[11]https://www.researchgate.net/publication/392368305_Measuring_the_Effectiveness_of_Cybersecurity_Training_Programs_in_SMEs

[12]https://www.nist.gov/publications/guide-integrating-forensic-techniques-incident-response

[13]https://standards.iteh.ai/catalog/standards/iso/3120680b-fb5d-4722-b2aa-71dd40e023a8/iso-iec-27035-4-2024

affected individuals.[14] There are also future potential disclosure obligations for which franchise systems need to maintain awareness and systems in place. For example, according to the Privacy Commissioner, records must be kept for all breaches, even those that do not have a risk of harm.[15]

For communicating with customers during cybersecurity incidents, clear and timely communication with affected individuals is critical to promote trust. External communications generally involve transparent and concise explanations of what happened and what data was affected, outlining steps taken to mitigate harm, and providing guidance on protective actions (e.g., credit monitoring and password changes).

Franchise systems add a layer of complexity. There should not be multiple (or, at worst, conflicting) communications from the franchise system. There should be a clear protocol in the franchise agreement and the franchise manual about who - typically the franchisor - should communicate to both regulators and the affected customers.

10.3 Cybersecurity Preparedness

Effective incident response is largely determined before an incident occurs. Organizations should maintain a formal incident response plan that defines roles and responsibilities, clarifies escalation procedures, and sets out communication workflows. For franchise systems operating in multiple jurisdictions, incident response will account for a nuanced response system that reflects the requirements in various legal and regulatory jurisdictions.[16] An important element of preparedness is regular testing through tabletop exercises, simulated cyber incidents, and post-incident reviews.

11. Insurance as a Risk Mitigation Tool

Insurance has always been a useful tool to manage all sorts of risks - the latest being cyber risks. Cyber insurance has evolved and has become an essential component of corporate risk management. For franchise systems, which face the layered exposures of network-wide operational disruption, multi-jurisdictional regulatory liability, and significant reputational risk, cyber insurance plays a genuinely important role in the risk management framework.

However, all insurance achieves is a transfer of financial risk and may offset financial loss and damage. It is not a substitute for robust cybersecurity practices and must be carefully integrated into broader risk strategies.

The scope of cover offered by cyber insurance policies has expanded considerably in recent years, though it remains variable across insurers and markets. A comprehensive cyber insurance policy may provide cover for:

- ***First-party losses***: Business interruption losses arising from a cyber incident, costs of forensic investigation, data restoration and system recovery, ransom payments (in jurisdictions where such payments are not prohibited), crisis communications and public relations support, and the cost of notifying affected individuals.

[14]https://laws-lois.justice.gc.ca/eng/acts/P-8.6/section-10.1.html

[15]https://www.priv.gc.ca/en/privacy-topics/business-privacy/breaches-and-safeguards/privacy-breaches-at-your-business/gd_pb_201810/

[16]https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management

- ***Third-party liability***: Claims brought by customers, employees, franchisees, or other third parties whose data was compromised, including defense costs and any damages awarded.

- ***Regulatory costs***: Legal costs associated with regulatory investigations and enforcement proceedings, and in some policies, fines and penalties (though coverage for regulatory penalties remains restricted in many jurisdictions due to public policy considerations).

- ***Extortion and ransom***: Coverage for the cost of managing ransomware incidents, including negotiation support and ransom payments where legally permissible.

  CAUTIONARY NOTE: While cyber insurance policies may provide coverage for 'extortion' or 'ransom' payments, such coverage does not alleviate the legal risks associated with international sanctions. In the United States, the Office of Foreign Assets Control (OFAC) prohibits transactions with individuals or entities on the Specially Designated Nationals (SDN) list. Under a strict liability standard, a franchisor or franchisee may be held civilly liable for a ransom payment to a sanctioned entity - such as certain state-sponsored hacking groups - even if they were unaware of the attacker's identity. Violations can result in multi-million dollar fines and criminal prosecution, regardless of whether the payment was funded by an insurer. Consequently, any decision to facilitate a ransom payment must be preceded by a thorough sanctions screening and immediate consultation with legal counsel and law enforcement (e.g., the FBI or CISA) to mitigate potential regulatory enforcement.

- ***Incident response services***: Some policies provide access to panels of pre-approved incident response providers forensic investigators, legal counsel, crisis communications specialists - which can be invaluable in the first hours and days of a significant incident. Insurers can now provide "24/7 follow-the-sun support" with cyber security experts, incident responders, and cyber claims adjusters. They are accessible through a response app, phone, email, and online experienced specialized teams. They also have the ability to partner with trusted vendors to assist with getting networks back online.

For franchise systems, the insurance should reflect the needs of the franchise system, and the underwriting process often forces better controls and visibility, adding significant value to a franchise system. The underwriting process conducted by cyber insurers has become increasingly rigorous. Insurers want to understand:

- The franchise system's security posture in detail;
- What controls are in place;
- What governance processes exist;
- What training is provided;
- What third-party risk management looks like; and
- What the incident response plan says.

The process associated with answering these questions often reveals gaps that the franchise network was not previously aware of. The underwriting process also functions as an independent security audit, and the improvements made to qualify for coverage are themselves valuable risk mitigation measures.

Insurers typically require, as conditions of coverage or as a basis for premium calculation:

- Multi-factor authentication (MFA) on all remote access points and privileged accounts, with some insurers now extending this requirement to all email access;
- Endpoint detection and response (EDR) capabilities on all systems;
- Regular, tested, offline backups of critical data and systems;
- A documented and tested incident response plan;

- Documented security awareness training, including phishing simulation exercises;
- Patch management processes meeting defined minimum standards; and
- Privileged access management and appropriate segregation of duties.

Franchise systems that cannot demonstrate such controls may not be able to obtain cyber insurance or may face substantially higher premiums and more restrictive policy terms. This creates a useful incentive alignment: insurers are, in effect, setting minimum security standards as a condition of financial protection. Franchise lawyers should bear this in mind and factor it into advice on both risk management and franchise agreement drafting and compliance obligations.

There are also important limitations and caveats that must be clearly communicated to franchisors:

First, the dramatic increase in ransomware incidents and the scale of losses in major incidents have led to substantially increased premiums, reduction of coverage limits, and more extensive exclusions. In particular, the insurance market has seen:

- War and nation-state exclusions to cyber claims. As a result, franchise systems operating in geopolitically sensitive regions may have limited or no coverage.
- The imposition of sub-limits on ransomware-related claims that are significantly lower than the overall policy limit, reflecting the frequency and severity of ransomware incidents.
- Systemic risk aggregation: insurers have become increasingly concerned about the aggregation of systemic cyber risk - scenarios in which a single attack affects thousands of policyholders simultaneously. This concern is directly relevant to franchise networks, where a single vendor compromise or central system breach can affect the entire portfolio. Franchise systems should understand how their insurer models this risk and what coverage implications it has.

Second, coverage is only triggered where the claim falls within the policy terms and conditions. Common bases for insurers to deny or reduce cyber claims include failure to maintain the security controls represented at the time of underwriting, failure to notify the insurer within the required timeframe, prior known incidents or circumstances not disclosed, and application of policy exclusions. Franchisors must review policy terms carefully and ensure that they understand insurance coverage and seek specialist legal and financial advice.

Third, and perhaps most importantly, insurance is not a “silver bullet” and does not prevent breaches. A franchise system that relies on insurance as its primary cyber risk management tool, rather than investing in prevention, good governance, and training of employees and franchisees, is misunderstanding both the purpose and the limitations of insurance. Insurance offsets financial loss after an incident has occurred. It does not protect the franchisor’s brand, does not preserve the trust of customers and franchisees, and does not prevent the operational disruption that can force franchise operations to cease. Prevention remains, by a significant margin, more valuable than any insurance policy.

The appropriate framing for franchise systems is this: cyber insurance is a necessary but not sufficient component of a comprehensive cybersecurity risk management program. It should be obtained, maintained, and regularly reviewed to ensure it remains adequate for the evolving risk profile of the franchise network. It must sit alongside, and is not a substitute for, robust technical controls, sound data governance, strong contractual frameworks, ongoing training, and tested incident response capability.

The key message is to be strategic about insurance - it is not a financial savior.

12. Conclusion

Cybersecurity within franchise systems has evolved beyond a purely technical concern into a multidimensional legal, operational, and governance challenge. The interconnected architecture of franchise networks creates systemic vulnerabilities in which weaknesses at a single franchisee, vendor, or internal access point may expose the broader network to substantial financial, regulatory, and reputational harm. As cyber threats continue to increase in sophistication and frequency, reactive approaches to cybersecurity are no longer sufficient.

This paper has demonstrated that effective cybersecurity governance in franchise systems requires a comprehensive and proactive framework integrating contractual regulation, technological controls, regulatory compliance, operational oversight, and human risk management. Particular importance must be placed on standardized cybersecurity obligations across franchise networks, cross-border incident preparedness, third-party risk management, and ongoing employee and franchisee training. Ultimately, cybersecurity resilience in franchise systems depends not merely on technological investment, but on the successful integration of law, governance, and operational practice. Franchise systems that fail to adopt such integrated approaches may face significant legal exposure and systemic disruption, whereas those that embed cybersecurity into the core structure of network governance will be better positioned to protect their operations, data integrity, and brand reputation in an increasingly digital commercial environment.

BIOGRAPHIES

ESMARI JONKER

Esmari heads the franchising law portfolio at Smit & Van Wyk Inc. in Pretoria, South Africa. She is a practising attorney, holding LLB and LLM degrees. Her practice focuses on intellectual property law and she has extensive experience in trade marks, copyright, unlawful competition, passing-off and franchise matters. Esmari advises both local and international clients in the franchise industry, acting for franchisors and franchisees in relation to franchise agreements, disputes, and related legal commercial matters. Her expertise further includes trade mark prosecution and litigation, copyright matters, commercial agreements, and High Court litigation involving intellectual property and franchise law.

After being admitted as an attorney of the High Court of South Africa in 2001, Esmari held senior positions at prominent law firms in South Africa before establishing the trade mark and franchise divisions at Smit & Van Wyk Inc. She also serves on the Membership Committee of the Franchise Association of South Africa (FASA).

Esmari has received significant recognition in the legal industry for her work in franchise and intellectual property law. She has been recognised by Best Lawyers for Franchise Law in South Africa and received the "Lawyer of the Year" award for Franchise Law in 2014. She has also been listed by Who's Who Legal in the Franchise Law category for South Africa, recognised by World Trademark Review 1000 as a recommended expert in trade mark prosecution and strategy, and received multiple Lexology Client Choice Awards.

GUSTAVO ALCOCER

Gustavo is a senior partner at OLIVARES, where he heads the corporate and commercial practice and co-chairs the firm's data privacy, new technologies, and life sciences groups. With more than 35 years of experience in private practice and in-house roles, he is widely regarded for his strategic counsel on complex, high-value transactions in Mexico and across jurisdictions.

His practice focuses on M&A, finance, and cross-border transactions, with particular strength in IP-intensive sectors, franchising, distribution, and supply chain structures. He regularly advises multinational corporations and investors on market entry, structuring, and expansion in Mexico, as well as on the valuation and monetization of assets and operations. Clients value his ability to combine technical precision with commercially driven, solution-oriented advice.

Gustavo has led and advised on numerous sophisticated transactions involving international stakeholders, guiding clients through regulatory, operational, and strategic considerations in dynamic and highly regulated industries.

He holds law degrees from Universidad Intercontinental and Universidad Nacional Autónoma de México (UNAM), and completed graduate studies at Fordham University School of Law. He is an active member of ANADE, the Barra Mexicana de Abogados, the American Bar Association, the International Association of Privacy Professionals, and the International Bar Association. Gustavo is fluent in English and Spanish and serves on the boards of several companies in Mexico and internationally, including the NMDP Foundation.

DOMINIC MOCHRIE

Dominic is acknowledged as a leading franchise lawyer in Canada. Dominic focuses on franchise and distribution, product marketing law and trade practice law. He provides practical and business-friendly advice to clients engaged in distribution and franchising matters, from start-up franchisors working to establish a new franchise system, to large, multi-national franchisors with thousands of franchisees. Dominic also supports clients in respect of various trade practice matters, including consumer protection, retail and marketing matters.

Dominic has extensive experience in wide variety of franchise systems, including hotel/hospitality franchises and retail fuel operations. Dominic also provides strategic advice to franchisors on franchising matters in M&A transactions, including advice on deal structure, risk analysis and risk mitigation. He has also recently assisted several franchisors “clean up” their franchise system prior to sale.

Dominic is actively in industry events and associations. He has been on many planning committees for the Canadian Franchise Association, the American Bar Association, the International Franchise Association, and the Ontario Bar Association. He is a frequent speaker and writer, including co-chairing the 2015 Ontario Bar Association’s Franchise Law Conference, presenting at the American Bar Association’s Forum on Franchising, and presenting at the International Franchise Association’s Legal Symposium. Dominic is also the International Distribution Institute’s designated franchise country expert for Canada. Dominic is ranked in Chambers Canada, Best Lawyers, Lexpert, Who’s Who Legal (Global): Franchise, Who’s Who Legal: Canada (Franchise), and is recognized as a “Legal Eagle” by Franchise Times.

RAYNIA THEODORE

Raynia is acknowledged as one of Australia's leading franchise lawyers, having focused her practice in the franchise sector for more than 25 years. She is a Principal at MST Lawyers - one of Australia's leading franchising and commercial law firms - where she leads the specialist franchise team, with expertise spanning franchising, commercial and leasing law. Raynia was named the 2026 Best Lawyers "Lawyer of the Year" for Franchise Law in Melbourne, an honour awarded to only one lawyer in each practice area and region based on peer review, and is recognised by Who's Who Legal as an "excellent" and "highly respected" franchising practitioner.

Raynia's extensive practice is dedicated to advising franchisors, franchisees and suppliers to the franchise sector on all aspects of franchising. She acts for many well-known national retail chains and franchise brands across a variety of industries, for new and emerging systems, and for international franchisors expanding into the Australian market. Raynia acts for clients (including franchisees and master franchisees) looking to acquire or dispose of franchise networks and franchises. Her clients seek advice on matters pertaining to franchising code compliance, franchise documentation, sales, purchases and restructuring of franchised systems/businesses and dispute resolution both in Australian and international jurisdictions. She also advises on competition and consumer law compliance - including pricing and supply issues, misleading or deceptive conduct, unconscionable conduct and good faith claims - and regularly deals with the Australian Competition and Consumer Commission. Raynia has extensive experience in retail and commercial leasing, with an intimate knowledge of retail legislation in all Australian states. Raynia is a member of the legal committee of the Franchise Council of Australia and is a regular presenter at the Legal Symposia held at the Franchise Council of Australia's national annual conventions. She is also a frequent commentator and author on franchise law developments, including Franchising Code reforms, ACCC enforcement activity and competition and consumer law issues affecting franchise networks.

EXHIBIT A

YEAR	COMPANY	TYPE OF ATTACK	HOW THEY ATTACKED	KEY ECONOMIC AND SOCIAL IMPACT
2013	Target Corporation	Third-Party Breach	Attackers compromised credentials of a third-party HVAC vendor with access to Target's network, moved laterally into the POS environment and installed malware to capture payment card data.	Data breach affecting +/- 40 million cards; losses exceeding USD 200 million; litigation and regulatory scrutiny. *https://akimbocore.com/article/target-breach-2013/*
2014	Domino's Pizza	Customer Database Breach / Extortion	Hackers infiltrated customer databases affecting operations in France and Belgium and threatened publication of stolen information unless ransom demands were met.	Exposure of data relating to over 600,000 customers; extortion demands; reputational damage and consumer distrust. *www.theguardian.com/technology/2014/jun/16/dominos-pizza-ransom-hack-data*
2015-2016	Hyatt Hotels Corporation	Malware Intrusion	Attackers installed malware on payment processing systems to capture customer cardholder data.	Exposure of customer financial data; remediation costs; reputational impact in the hospitality sector. *www.sbs.com.au/news/article/hyatt-hotels-attacked-with-malware/l5r2og1xx* *https://abcnews.com/Technology/hyatt-reveals-data-breach-impacted- 250 hotels/story?id=36315368*
2016 - 2019	The Wendy's Company	Malware / POS Breach	Attackers infiltrated franchisee systems and deployed malware on point-of-sale infrastructure to capture payment card data over an extended period.	Large-scale payment data theft; class actions; financial and reputational harm. *www.wendys.com/payment-card-incident*

2018	British Airways plc	Web Skimming (Magecart)	Attackers injected malicious JavaScript into the airline's website and mobile application to intercept payment details in real time.	+/- 400,000 customers affected; regulatory fines and severe reputational consequences. *www.theguardian.com/business/2019/jul/08/ba-fine-customer-data-breach-british-airways*
2019	Petróleos Mexicanos (PEMEX)	Ransomware	Threat actors used spear-phishing emails and malicious attachments to compromise systems, escalate privileges and encrypt critical infrastructure.	Operational disruption; inability to process payments; ransom demand reportedly around USD 5 million. *www.cybersaint.io/news/mexican-state-owned-petroleum-firm-pemex-crippled-by-ransomware*
2019 - 2025	Chipotle Mexican Grill, Inc.	Account Takeover / Credential Stuffing	Attackers used automated credential stuffing attacks with previously leaked usernames and passwords to compromise customer accounts.	Fraudulent transactions; erosion of customer trust; increased cybersecurity expenditure. *www.fastcasual.com/news/hackers-target-chipotle-customers-in-credential-stuffing-attack/* *https://thelyonfirm.com/blog/chipotle-data-breach-investigation/*
2021	McDonald's	Global Data Breach	Hackers gained unauthorised access to internal systems and extracted customer and employee data from multiple jurisdictions.	Exposure of employee and customer information across the United States, South Korea and Taiwan; compliance and notification obligations. *www.wsj.com/tech/cybersecurity/mcdonalds-hit-by-data-breach-in-south-korea-taiwan-11623412800*
2022	Uber Technologies Inc.	Social Engineering	Attackers used stolen credentials and MFA fatigue techniques to gain privileged access to	Broad compromise of internal systems; operational disruption; highlighted weaknesses

			internal systems and administrative tools.	in identity and access management. *https://techcrunch.com/2022/09/16/uber-internal-network-hack/*
2023	Yum! Brands (KFC, Pizza Hut, Taco Bell)	Ransomware	Ransomware actors disrupted IT infrastructure used by franchise operations, resulting in service interruptions and temporary closures.	+/- 300 restaurants in the United Kingdom temporarily closed; operational and financial losses. *www.yum.com/wps/portal/yumbrands/Yumbrands/news/company-stories/Yum%21+Brands+May+18%2C+2023+Statement*
2023	Caesars Entertainment	Social Engineering / Ransomware	Threat actors manipulated IT help desk procedures and obtained access to customer loyalty databases before extortion demands were issued.	Exposure of customer loyalty data; reported ransom payment of approximately USD 15 million. *https://digiknow.dti.delaware.gov/news/contentFolder/pdfs/newsletters/202310_eSecurityNews.pdf*
2023	MGM Resorts International	Social Engineering Cyberattack	Attackers compromised IT systems through social engineering techniques, causing prolonged outages across hotel, casino and reservation systems.	Operational shutdowns for several days; estimated losses of approximately USD 100 million. *westoahu.hawaii.edu/cyber/global-weekly-exec-summary/alphv-hackers-reveal-details-of-mgm-cyber-attack/*
2024	Coppel	Ransomware	Attackers allegedly 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. *www.cyberpeace.tech/post/as%C3%AD-fue-el-hackeo-que-sufrio-*

				coppel-y-que-afecto-1800-tiendas
2024	Subway	Ransomware Threat / Data Theft	The LockBit ransomware group claimed to have infiltrated company systems and threatened publication of allegedly stolen data.	*Potential exposure of corporate and customer data; reputational and operational risk.* *www.securityweek.com /sandwich-chain-subway-investigating-ransomware-groups-claims/*
2024	Ultra Tune (Australia)	Alleged Ransomware / Data Theft	The Fog ransomware group allegedly exfiltrated approximately three gigabytes of data including HR records, customer information and internal databases.	Exposure of passports, driver's licences, medical certificates and employee information; reputational and regulatory risk. *www.cyberdaily.au/ security/11264-exclusive-major-australian-mechanic-ultratune-suffers-alleged-cyber-attack*
2025	Restaurant Brands International	Platform Vulnerabilities	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. *www.malwarebytes.com/ blog/news/2025/09/popeyes-tim-hortons-burger-king-platforms-have-catastrophic-vulnerabilities-say-hackers*
2025	Wynn Resorts	Credential Compromise / Data Breach	Attackers allegedly compromised employee credentials and accessed human resources and payroll information.	Exposure of employee salary, HR and contact information; reputational and compliance implications. *https://consumer.zlk.com/ data-breach/wynn-resorts-ltd-data-breach/*
2026	Starbucks	Phishing Attack	Attackers used fraudulent HR portals to harvest employee	Compromise of employee login details and payroll-related data; increased phishing and fraud risk.

			credentials and payroll information.	*https://shieldworkz.com/blogs/inside-the starbucks-breach-trilogy*
May 2026	Instructure / Canvas LMS	Data Breach / Cyber Extortion / Ransomware	Attackers exploited vulnerabilities associated with Canvas 'Free-for-Teacher' accounts and related infrastructure to obtain access to user data, internal communications and institutional systems. Attackers defaced login portals, disrupted services during examination periods and threatened publication of stolen data unless ransom demands were met.	Reported impact on approximately 275 million users across nearly 9,000 educational institutions worldwide; disruption of examinations and academic operations; exposure of names, email addresses, student numbers and communications; potential litigation, regulatory scrutiny and reputational damage. *www.npr.org/2026/05/08/nx-s1-5815956/canvas-data-breach-school-finals* *https://usaherald.com/hackers-breach-canvas-platform-exposing-data-of-30-million-students-platform-goes-dark-during-finals-week/* *https://www.k12dive.com/news/a-2nd-canvas-data-breach-causes-major-disruptions-for-schools-colleges/819755/*

EXHIBIT B

Glossary of Cybersecurity Terms

TERM	DESCRIPTION
Malware	Malicious software designed to damage, spy on, or take control of computer systems without authorization.
Virus	A type of malware that attaches itself to files and spreads when users execute them.
Worm	Malware that automatically spreads across networks without user interaction.
Trojan (Trojan Horse)	A program that appears legitimate but creates unauthorized access for attackers once installed.
Ransomware	Malware that encrypts data and demands payment to restore access.
Phishing	An attack using fake emails, messages, or websites to trick users into revealing sensitive information.
Spear Phishing	A targeted phishing attack aimed at a specific individual or department using personalized information.
Whaling	A phishing attack specifically targeting executives or high-level personnel.
Smishing	Phishing conducted through SMS or messaging apps such as WhatsApp.
Vishing	Phishing carried out through phone calls.
Spyware	Malware that secretly collects user information without their knowledge.
Adware	Software that displays unwanted advertisements and may track browsing activity.
Keylogger	A tool that records keystrokes to capture passwords and sensitive information.
Backdoor	A hidden method of bypassing security to gain unauthorized remote access to a system.
Botnet	A network of infected devices controlled remotely to perform large-scale attacks.
DDoS (Distributed Denial of Service)	An attack that overwhelms a system or service with traffic to make it unavailable.
Man-in-the-Middle (MitM)	An attack where a third party intercepts communication between two parties.

TERM	DESCRIPTION
Credential Stuffing	The use of stolen credentials from other services to gain unauthorized access to systems.
Brute Force Attack	An attack that attempts multiple password combinations until the correct one is found.
Zero-Day	A previously unknown vulnerability for which no security patch exists.
Exploit	Code or a technique used to take advantage of a vulnerability to carry out an attack.
Privilege Escalation	A technique where an attacker gains higher-level permissions within a system.
Social Engineering	Psychological manipulation used to deceive individuals into revealing confidential information or granting access.
Data Breach	Unauthorized exposure or theft of sensitive information.
Insider Threat	A risk originating from employees or third parties with legitimate system access.
Shadow IT	The use of unauthorized applications or services outside the control of the IT department.