ofi

Strategic Threat Landscape Briefing: Securing ofi's Global Value Chain

An analysis of ofi's attack surface and critical vulnerabilities to inform a robust, intelligence-led cybersecurity strategy.

ofi is a Global Leader, and Leadership Attracts Advanced Threats

- **A Powerhouse in Global Ingredients:** ofi operates at a significant scale with **S$12.6 billion** in revenue, driven by strong positions in cocoa, coffee, dairy, nuts, and spices.
- **Deeply Integrated Value Chain:** From plant science and farmer engagement to global processing and customer co-creation, ofi's model is built on an intricate physical and digital infrastructure.
- **The Strategic Imperative:** This briefing maps ofi's expanding operational footprint—its "attack surface"—to identify the most critical cyber threats to its business continuity, intellectual property, and reputation.
- **Our Objective:** To provide the foundational business intelligence required to scope a targeted, in-depth technical vulnerability assessment using frameworks like MITRE ATT&CK.

Defining Our Crown Jewels: What We Must Protect at All Costs

Operational Technology (OT) & Manufacturing

The continuous operation of 145+ processing facilities worldwide. Disruption here means immediate revenue loss and potential safety incidents.

Supply Chain Integrity Integrity & Data

The trust and traceability built into our platforms like AtSource and TRACT. Data corruption erodes customer confidence and risks regulatory non-compliance (e.g., EUDR).

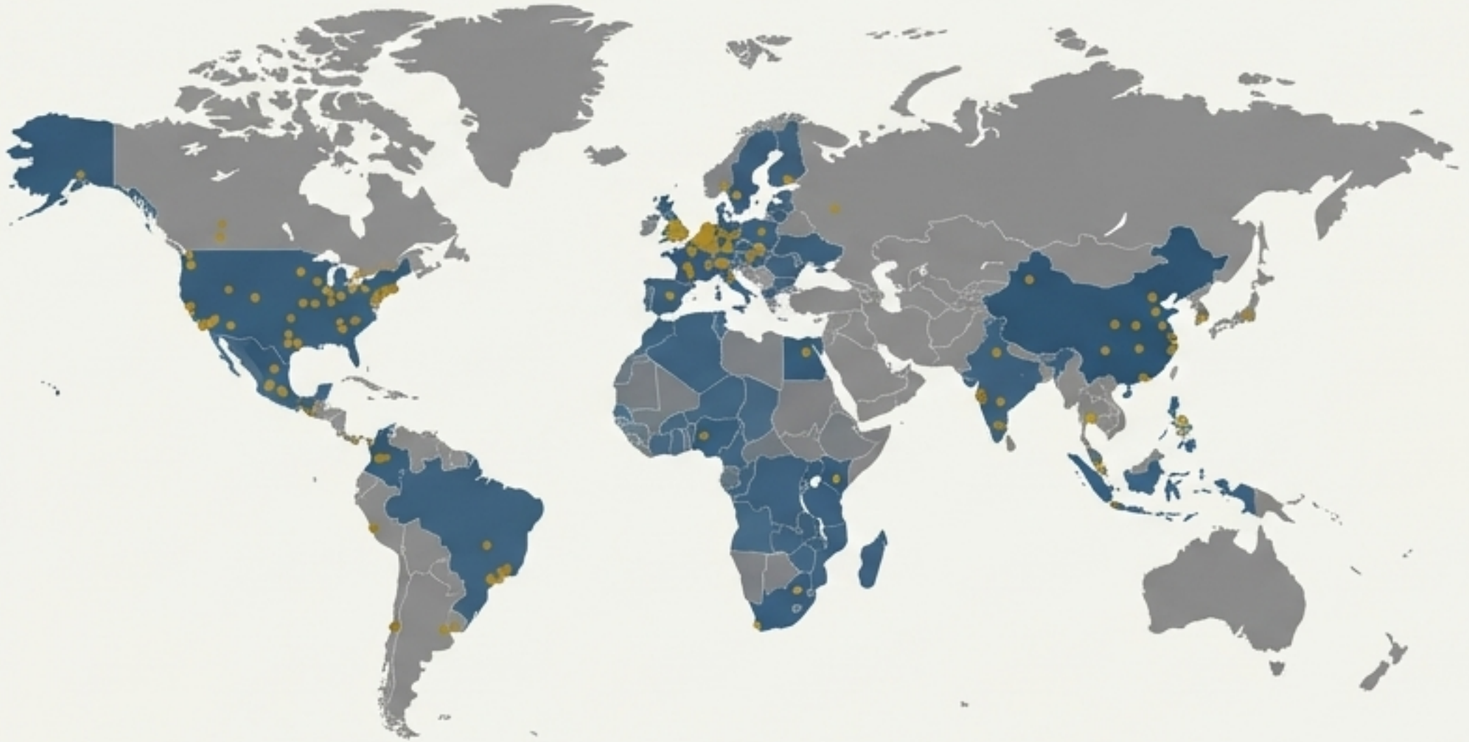
Intellectual Property (IP) & Innovation

Proprietary plant science, product formulations from our five Customer Solutions Centres, and sensitive R&D data.

Farmer & Partner Ecosystem Data

Vast datasets on millions of farmers and thousands of partners via apps like OFIS and Jiva's AgriCentral. A breach risks massive reputational damage and PII liability.

A Sprawling Global Footprint Creates 145+ Potential OT Entry Points



39 Tier 1 (Large Manufacturing) Plants

123 Tier 2 (Primary Processing) Plants

180 Tier 3 (Warehouses)

Total Facilities Assessed

The source data confirms 145 ofi processing sites were assessed for biodiversity risk, with 74 located within 10km of a Protected Area and 59 considered medium or high risk.

Our operational backbone consists of a vast network of processing plants, manufacturing facilities, and warehouses. Each site represents a potential entry point for threats targeting Operational Technology (OT). An attack on these facilities could halt production, compromise food safety, and create physical safety hazards.

‘We improved the global auditing programme for safety, serious injury and fatality assessments in all our sites, which has driven improvements in safety culture and leadership.’

The Digital Nervous System: A Hyper-Connected ‘Farm to Fork’ Ecosystem

Farm

OFI Farmer Information System (OFIS) & ofi Direct

App. Collecting GPS locations, yields, and transacting directly with farmers.

Supply Chain

Track and Trace System & AtSource Platform

Integrating field apps with ERP systems for end-to-end visibility and sustainability verification (EUDR).

Customer

F&B Solutions Platform & 5 Global CSCs

Co-creating new products with partners, sharing sensitive R&D and consumer insights.

ofi's competitive edge is driven by 'Supply Chain 4.0'—a vision of extensive automation, IoT, and big data analytics. While powerful, this integration creates a **single, contiguous digital attack surface** where a breach in one area can cascade across the entire value chain.

The Farmer Data Nexus: A High-Value Target for Data Theft and Misuse

11,000,000+

- Jiva's AgriCentral farmer application has over **11 million registered farmers** in India, featuring AI-driven pest and disease diagnosis tools.
- ofi's proprietary **OFIS** app is a survey tool built to bridge digital gaps, collecting farm GPS locations, yields, and community information, even from farmers lacking internet connections.
- The '**ofi Direct**' app enables direct farmer transactions, giving farmers access to advice, financing, and supplies while digitally tracing crops.

Cybersecurity Implication:

This concentration of Personally Identifiable Information (PII) and sensitive operational data is a prime target for threat actors. A breach would result in severe regulatory penalties (e.g., GDPR), loss of farmer trust, and significant brand damage. The offline capabilities of OFIS present a unique data synchronization risk.

Guarding the Innovation Engine: Protecting High-Value Intellectual Property

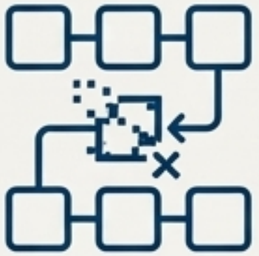
- **Co-Creation is Core to the Business**: The F&B Solutions platform and five Customer Solutions Centres (Amsterdam, Bangalore, Chicago, Singapore, Shanghai) are where ofi partners with global brands like **Mars** and innovators like **iD Fresh Food** to develop new products.
- **Proprietary Science & Data:** ofi's competitive advantage lies in its deep expertise, such as the onion seed breeding program that improves yields and reduces water use. This proprietary plant science is invaluable IP.
- **Digital Tools & Analytics:** The development of platforms like the AI-powered Carbon Stock Monitoring tool and internal 'private AI' tools by Mindsprint represent significant R&D investment and house sensitive business logic.

Cybersecurity Implication: These collaborative and R&D environments are high-value targets for industrial espionage. A breach could lead to the theft of trade secrets, product formulations, and strategic plans, directly impacting future revenue and market position.

Synthesized Threat Vectors: The Four Critical Risks to ofi's Enterprise

Threat Vector 1: OT Disruption & Sabotage

- **Target:** 145+ global processing facilities.
- **Impact:** Production shutdown, supply chain paralysis, food safety crises, potential physical harm to employees.
- **Attacker Motivation:** Ransomware, nation-state disruption, competitor sabotage.



Threat Vector 2: Supply Chain Data Manipulation

- **Target:** AtSource, TRACT, and ERP systems.
- **Impact:** Loss of traceability, failure to meet EUDR compliance, destruction of customer trust, financial penalties.
- **Attacker Motivation:** Hacktivism, competitor sabotage, creating market chaos.

Threat Vector 3: Strategic IP Theft

- **Target:** Customer Solutions Centres, R&D data, F&B Solutions platform, proprietary algorithms.
- **Impact:** Loss of competitive advantage, erosion of market leadership, counterfeit products.
- **Attacker Motivation:** Industrial espionage by competitors or nation-states.

Threat Vector 4: Mass PII & Farmer Data Breach

- **Target:** OFIS, ofi Direct, AgriCentral applications.
- **Impact:** Massive regulatory fines, reputational collapse, loss of farmer engagement, class-action lawsuits.
- **Attacker Motivation:** Cybercrime (data for sale), hacktivism.

A Mature Governance Framework is in Place, But Technical Assurance is Key

Key Governance Points

- Cybersecurity is formally identified as a key risk, owned by the Audit and Risk Committee.
- A formal Whistleblowing Policy (“Speak Out!”) was rolled out globally in 2024.
- The Group employs IT security experts and cybersecurity infrastructure to mitigate risks.

The Mindsprint Paradox: A Strategic Asset and a Potential Concentration Risk

Asset

Deep Institutional Knowledge: "Unique experience and expertise...gained in navigating complex businesses and supply chains" within Olam Group.

Advanced Capabilities: Developing a "private AI tool...with more security," R&D focus, SAP Gold Partner.

Scale: Approximately 3,000 employees.

Risk

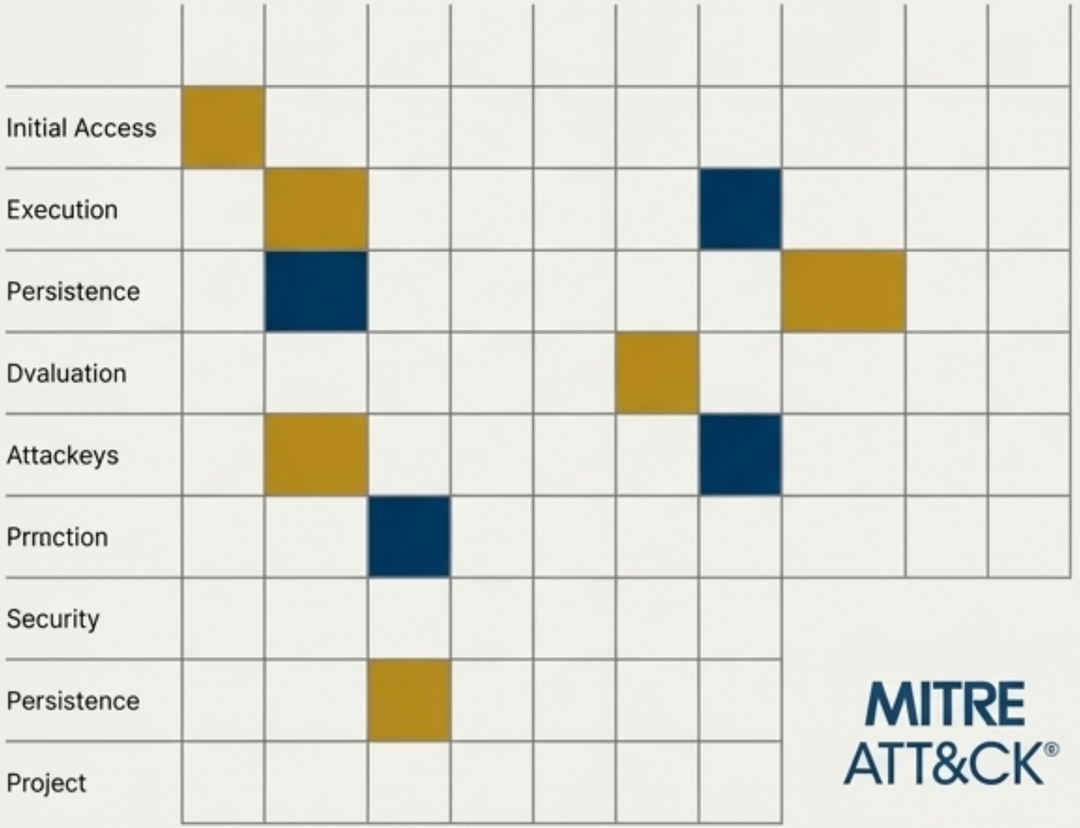
External Focus: Now carved out to "pursue contracts with third parties" in CPG, manufacturing, and life sciences.

Shared Infrastructure?: As Mindsprint serves external clients, are ofi's systems, data, and security teams adequately segregated?

Resource Allocation: Will ofi's security needs be prioritized against the demands of new, external customers?

Strategic Question: As Mindsprint expands its external client base, how do we ensure its security service delivery to ofi remains best-in-class, ring-fenced, and free from conflicts of interest?

The Path Forward: A Targeted Assessment Aligned to the MITRE ATT&CK® Framework



We have identified the strategic business risks. The critical next step is to understand how threat actors could technically execute attacks against our Crown Jewels. A formal assessment based on the MITRE ATT&CK framework will allow us to move from *what* is at risk to *how* it is at risk.

Proposed Assessment Focus Areas

1. **OT Network Security Review**: Penetration testing and architecture review of a representative sample of Tier 1 and Tier 2 processing facilities.
2. **Supply Chain Platform Security**: Code review and vulnerability assessment of the AtSource, OFIS, and Track and Trace platforms, focusing on data integrity.
3. **Cloud & Corporate Infrastructure Review**: Assess the security of the ERP systems, data lakes, and infrastructure housing R&D and farmer PII against common ransomware and data exfiltration TTPs (Tactics, Techniques, and Procedures).
4. **Partner Ecosystem Security**: Review security protocols for third-party collaboration in Customer Solutions Centres.

Profiling the Adversary: Who Targets a Global Agri-Business Leader?

Nation-State Actors

- **Motivation:** Industrial espionage to steal IP (plant science, formulations); geopolitical disruption of global food supply chains.
- **Likely TTPs:** Advanced Persistent Threats (APTs), supply chain compromise, targeting R&D personnel.

E-Crime Syndicates

- **Motivation:** Purely financial. Ransomware attacks on OT and IT systems; theft and sale of PII from farmer databases on the dark web.
- **Likely TTPs:** Phishing, exploiting known vulnerabilities, Ransomware-as-a-Service (RaaS).

Hacktivists & Insiders

- **Motivation:** To damage ofi's reputation based on its ESG leadership status; disgruntled employees seeking to cause harm.
- **Likely TTPs:** Website defacement, leaking sensitive internal documents, manipulating sustainability data in AtSource to cause reputational damage.

Recommended Actions & Roadmap

Next 30 Days

Phase 1: Scope & Mobilize

- Formally charter the MITRE ATT&CK-based technical assessment project.
- Finalize scope and select a third-party cybersecurity partner to work alongside Mindsprint, ensuring independent validation.
- Brief executive sponsors at the Audit and Risk Committee.

Months 2-4

Phase 2: Technical Assessment

- Execute the four-pronged assessment (OT, Supply Chain Platforms, Corporate IT, Partner Ecosystem).
- Conduct parallel tabletop exercises based on the key threat vectors (e.g., OT ransomware event, AtSource data integrity attack).

Months 5-6

Phase 3: Strategic Remediation Plan

- Analyze findings and map vulnerabilities to the IRAF.
- Develop a prioritized, budget-conscious remediation roadmap.
- Present final findings and strategic plan to the Board.

From Risk Awareness to Proactive Resilience

- ofi's global scale and deep digital integration are its greatest strengths and its most significant sources of cyber risk.
- The attack surface is vast, spanning from remote farms in emerging markets to sophisticated R&D centers in global capitals.
- Key threat vectors—OT disruption, IP theft, data manipulation, and PII breaches—pose a direct existential threat to core business operations.

A proactive, intelligence-led security posture is not merely a cost of doing business; it is a critical enabler of trust, innovation, and resilience. Investing in a deep understanding of our technical vulnerabilities is the essential next step to safeguarding ofi's future growth.