



***FORWARD
IN FOCUS***

Expanding the Attack Surface: Cyber Risk and Fraud in a Digitized Distribution Business

IFDA 2026 Solutions Conference | Share Group

Frank Smith





**Ten years ago, the attack surface was
basically the four walls of IT.**

Today, it is the business.



1. The New Attack Surface

Digitization rewired
distribution risk

What changes?

WMS, TMS, ERP, CRM, EDI and ordering platforms are all part of the perimeter.

Identity and integrations now matter as much as the traditional network.

Connected systems create efficiency — and new paths into the operation.

2. Third-Party Automation & Integrations

“Set it and forget it” can become standing risk

What changes?

APIs, RPA bots and scheduled feeds often use broad, persistent credentials.

Automation can multiply a mistake or exploit at machine speed.

A common gap: no clear owner for an integration or what it can access.

3. Remote Access, Mobile & the Extended Workforce

The warehouse, cab and
home office are all
connected

What changes?

Drivers, warehouse teams and hybrid employees depend on mobile and remote access.

Handhelds, scanners, telematics and contractor devices expand the number of footholds.

Shared devices and remote-support tools complicate patching, identity and access control.

4. Vendor & Partner Connectivity

Your trust boundary extends beyond your company

What changes?

EDI partners, suppliers, freight brokers and SaaS platforms may have direct business access.

Vendor access can persist long after roles or relationships change.

The partners that can reach systems or move money deserve the deepest scrutiny.

5. Data-Driven Processes & the Fraud Angle

Cyber risk and internal fraud increasingly share the same controls

What changes?

Ghost vendors, invoice fraud, payroll manipulation and unauthorized pricing can hide in complex workflows.

High-volume payments make fraudulent changes easier to blend into normal activity.

External attackers and insiders both benefit from excessive standing access and weak review.

6. What It Actually Costs the Business

A cyber incident does not stop at IT

What changes?

Order-to-cash can stop: ordering, picking, routing, shipping, invoicing and payment.

Operational disruption can mean spoilage, missed SLAs, penalties and customer churn.

Fraud can compound quietly for months before anyone knows the true loss.

7. Reduce Exposure Without Slowing the Business

Put controls where consequence justifies friction

What changes?

MFA, least privilege and segmentation reduce blast radius.

Tier vendor risk instead of treating every vendor the same.

Use dual approval for sensitive financial changes and scheduled access reviews.

Build security and fraud controls into automation from day one.

**What is one risk you had not fully
considered —
and one thing you will do differently?**