



Topic	Importance
Agentic AI / Agentic Commerce Security	AI agents are beginning to shop, transact, access systems and make decisions. Retailers have to distinguish legitimate agents from malicious bots.
Identity Is the New Attack Surface	Human identities + service accounts + vendors + customers + AI/non-human identities are converging.
Cyber + Fraud Convergence	Account takeover, loyalty fraud, refund fraud, synthetic identities and deepfake support calls increasingly cross traditional fraud/security boundaries.
AI-Powered Social Engineering	Deepfake voice/video, highly personalized phishing and help-desk attacks are particularly dangerous in hospitality and distributed retail.
Third-Party / SaaS / Supply-Chain Risk	Retail and hotels depend on enormous ecosystems of suppliers, franchises, booking platforms, payment processors and SaaS vendors.
Securing AI Itself	Shadow AI, data leakage, prompt injection, model access, AI governance and rogue agents.
Cyber Resilience vs. Cyber Prevention	Incident response, business continuity and keeping stores/hotels operating during an attack.
SOC Reinvention	AI-driven SOC, autonomous investigation, tool consolidation and the build/buy/outsource question.
API & Digital Commerce Security	APIs increasingly connect ecommerce, mobile apps, loyalty, reservations, payments and AI agents.
Cyber Deception	Deception is moving from experimental technology toward practical detection/defense.
OT/IoT + Physical/Digital Convergence	POS, kiosks, cameras, smart rooms, HVAC, locks, warehouses and connected stores/hotels.
Post-Quantum Readiness	Crypto inventories and migration planning are moving from theoretical conversations into actual programs.
Cyber Workforce Transformation	What security teams look like when AI agents perform Tier 1/Tier 2 analyst work.