trackforce®

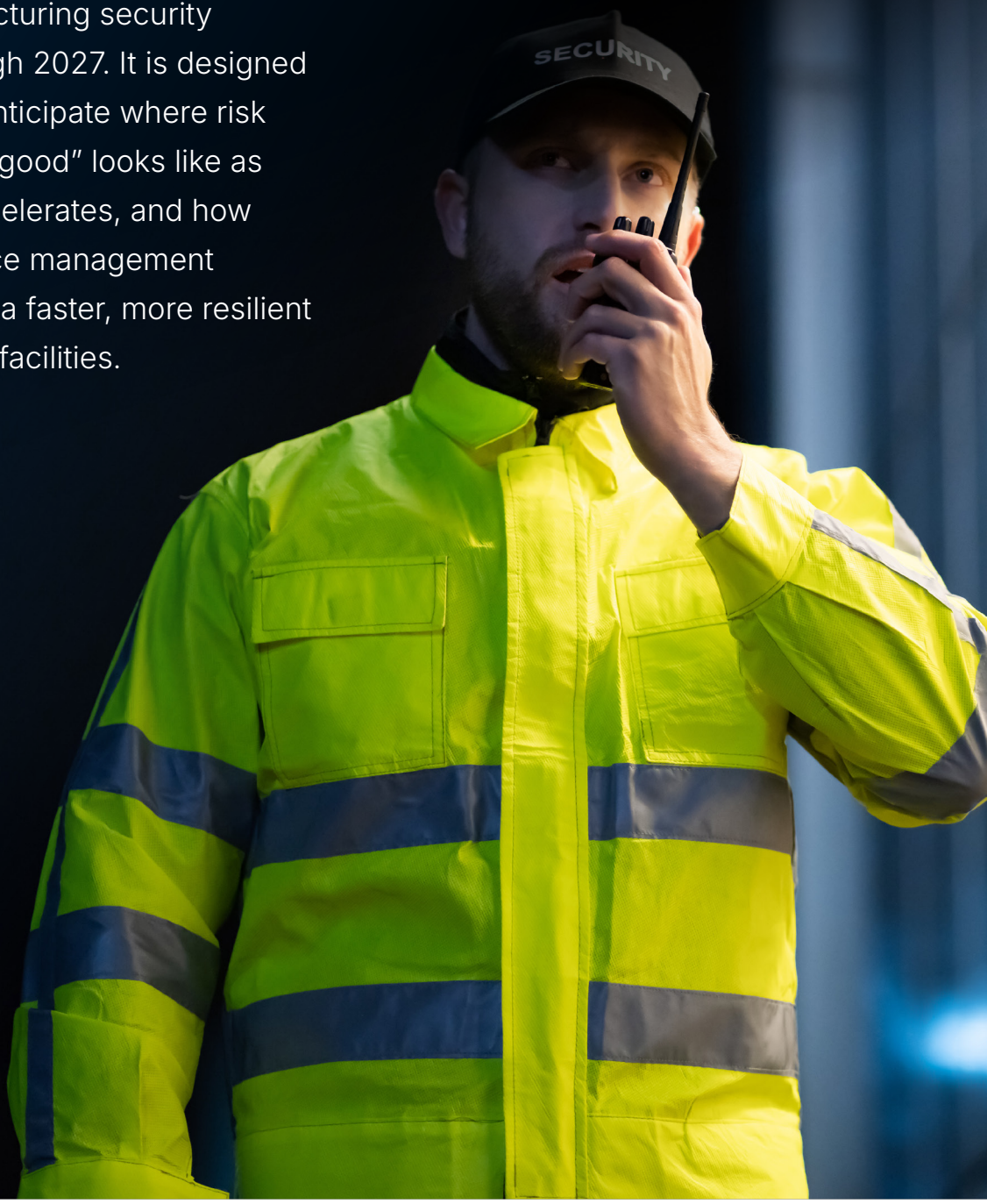
Cyber-Physical Security Convergence in Manufacturing

An Executive Trends Report
on Security and Operational Risk

Table of Contents

How To Read This Report

This predictive trends piece highlights five developments that are likely to shape manufacturing security operations through 2027. It is designed to help leaders anticipate where risk is moving, what “good” looks like as convergence accelerates, and how security workforce management platforms enable a faster, more resilient response across facilities.



Methodology and Scope

Findings are informed by qualitative interviews with Aaron Donnelly, a global security leader and former Regional WIM Manager at Amazon, Jeff Reinke, editorial director for Industrial Equipment News, Todd Kreisher, former head of security at BMW of Noth America, and Jon Black, SVP, Private Security Team at HUB International Insurance Services, plus supporting desk research and benchmark context as directional signal. The focus is cyber–physical convergence in manufacturing, including IT, OT or ICS, and networked physical security systems (access control, video, visitor workflows, and guard operations).

BASELINE

What Manufacturing Security Looks Like Right Now

Manufacturers are not starting from the same place. Reinke observes that large enterprises have addressed much of the “low hanging fruit” in basic cyber hygiene but still struggle with segmentation that does not disrupt production.

Smaller manufacturers often underestimate their risk and remain exposed through credential discipline, inconsistent access controls, and limited asset visibility. Across the board, Reinke estimates that 85% to 90% of organizations still operate in IT and OT silos, which slows coordination during incidents. Industry data reinforces why these gaps are not staying theoretical. IBM X-Force reporting shows manufacturing was the most attacked industry in 2024, accounting for 25.7% of incidents in its dataset.

Kreisher saw a similar, uneven starting line on the physical side. He described inheriting a program that relied heavily on outsourced coverage and inconsistent reporting, which made it difficult to brief leadership or spot patterns across incidents. Standardizing incident capture and making reports executive-ready improved visibility, supported faster decisions, and strengthened compliance documentation across a large site. Meanwhile, Donnelly warns that resilience is defined by whether organizations can keep operations safe and running when communications, staffing, and physical access are constrained.

Black adds that insurers are raising expectations around the operational evidence associated with security programs. Underwriters want time-stamped activity logs, standardized incident capture, and repeatable response protocols that show controls in practice, not just on paper. Negligence allegations often come down to evidence.

trackforce®

5 Predictive Trends

THROUGH 2027

TREND 1

Segmentation Becomes an Uptime-Linked Business Control

Segmentation is the control that determines whether an incident stays contained or becomes an operational event. Reinke said larger enterprises have improved basic controls but still struggle with “understanding how to cut things off” without risking uptime or slowing production.

Public data points in the same direction. Manufacturing remains a top target in sector reporting, and ransomware is persistent because disruption creates leverage. FBI reporting shows ransomware complaints rising across U.S. critical infrastructure, including manufacturing. The FBI’s Annual Internet Crime Report describes ransomware as the most pervasive critical infrastructure threat and reports complaints rose 9% year over year, keeping pressure on segmentation and recovery practices that reduce downtime exposure. Honeywell reported a jump in ransomware activity targeting industrial operators in early 2025, alongside a surge in malware designed to steal industrial credentials. Segmentation decisions will be judged by downtime avoided and recovery speed.

That standard is also showing up in risk financing conversations. Insurers increasingly ask for evidence that segmentation limits blast radius and supports repeatable recovery, not just policy-level intent. When organizations are unable to demonstrate how disruptions are contained, downtime exposure becomes harder to defend and more costly to insure.

RECOMMENDED MOVES

include maintaining a living OT asset inventory, mapping critical dependencies, and phasing segmentation changes with OT input. Watch for segmentation programs tied to uptime metrics and aligned to ISA/IEC 62443 zoning principles.

TREND 2

Identity Discipline Expands to Contractors, Visitors, and Remote Access

Hybrid incidents often begin with access that looks routine until it's correlated. Reinke sees smaller manufacturers underestimate exposure because they assume they are "too small to be targeted," which leaves gaps in credential discipline and offboarding. Privilege creep on contractor badges, shared accounts, and remote support credentials that are not time-bounded create physical-to-digital pivot points.

Kreisher described a common enterprise failure mode. Large organizations drift into inconsistent access practices across sites unless identity is governed as one lifecycle and audited against a common standard. Through 2027, manufacturers will connect badge provisioning, visitor approvals, and contractor windows to digital privileges so one identity has one risk profile.

From an insurance standpoint, third-party identity sprawl is treated as a measurable control gap. Clear, auditable lifecycle controls, such as time-bounded access, consistent offboarding, and standardized exceptions, strengthen defensibility after incidents and reduce friction during policy renewals.

RECOMMENDED MOVES

include MFA where feasible, eliminating shared credentials, tightening offboarding timelines, and reviewing contractor access on a cadence. Watch for tighter links between physical credentialing and IAM systems and for investigations that reference valid credentials or unmanaged devices.

TREND 3

Convergence Succeeds or Fails at Handoffs, Ownership, and Visibility

Convergence fails most often at handoffs. Reinke estimated that IT and OT still operate in silos most of the time, and he hears vendors being asked to “bring IT and OT into the same room.” Without a shared operating model, incidents trigger stalled decisions and slow handoffs because OT is measured on uptime and IT on risk reduction.

NIST
National Institute of Standards and Technology

NIST Cybersecurity Framework 2.0 elevated governance through a new “Govern” function, reinforcing the need for clear ownership and decision rights. Manufacturers that recover faster tend to have a shared severity language, defined escalation paths, and rehearsed incident command that includes IT, OT, facilities, and physical security.

Those governance and handoff mechanics are also what carriers examine when evaluating whether response procedures are repeatable across sites. When escalation paths and documentation vary by facility, it’s harder to show consistent execution after an event, and harder to defend outcomes under a duty-of-care lens.

RECOMMENDED MOVES

include cross-domain playbooks, defined ownership for hybrid events, and measured time-to-escalate and time-to-triage. Watch for steering groups and joint exercises that include operations, facilities, and safety.

TREND 4

Physical Security Systems Are Treated as Cyber Assets

Cameras, access controllers, and visitor tools are now part of the attack surface when they sit on networks and store credentials. Black notes carriers evaluate these systems through a cyber lens, looking for evidence of credential discipline, access audit trails, and device posture documentation.

Reinke notes that many manufacturers still treat these systems as facilities-only tools, even though cameras and electronic doors can be hacked when tied into broader systems. That gap matters because manufacturing incidents are measured in downtime and safety risk, not just data loss.

Safe operations planning belongs in the same conversation. By 2027, leading manufacturers will manage physical security devices like other critical assets, including inventory, hardening, segmentation, and log forwarding. CISA guidance on protecting network edge devices and ISA or IEC 62443 both reinforce that direction.

WHAT TO WATCH

includes firmware and credential management programs, segmentation for security infrastructure, and logs flowing into enterprise workflows. What to do now includes removing default credentials, validating configurations, segmenting device networks where feasible, and standardizing incident documentation so physical events can be correlated with cyber and OT indicators.

TREND 5

Resilience Shifts Toward Continuity Execution and Automated Communications

Recovery is becoming the differentiator. Reinke notes that stopping an attacker is “only half the battle” without response plans for breach, malware, and ransom scenarios. In industrial environments, delayed recovery can create safety hazards, compliance exposure, and uncontrolled downtime when plants cannot quickly verify which systems, zones, and access methods are safe to operate.

Donnelly adds that continuity pressure often hits people and communications as much as systems. Severe weather can displace guards and critical staff, while regional power outages can degrade connectivity for cameras, badge systems, and monitoring. Supply chain shocks can also spike contractor and delivery volume, raising the importance of time-bounded credentials, rapid identity verification, and consistent logging across sites.

Recent natural disasters and regional infrastructure outages reinforce that disruption often begins with communication breakdown, not malware. When employees are displaced or internet access is limited, plants struggle to confirm workforce availability, verify site status, and coordinate response across distributed facilities. Through 2027, manufacturers will invest more in degraded-mode procedures, crisis communications automation, and repeatable site-level process discipline.

That scrutiny is tied to real loss exposure beyond extreme-weather events. The National Fire Protection Association (NFPA) estimates U.S. fire departments respond to an annual average of 36,784 fires at industrial or manufacturing properties, with $1.5 billion in direct property damage annually. That’s part of why carriers are pushing harder for documented controls and repeatable response procedures.

In many manufacturing losses, liability turns on documentation: whether post orders were followed, whether patrols occurred, whether a contractor was properly badged/offboarded, and whether deviations were escalated. When those records are inconsistent across sites, carriers face a weaker defense posture.

WHAT TO WATCH

defined degraded-mode triggers and safe-operating thresholds, mass-notification tooling, site-status verification processes, and drills that test limited-connectivity scenarios.
What to do now: keep employee contact data current across systems, test communications under constraint, and document each facility’s minimum safe operating posture.

What Convergence Looks Like in 2027

By 2027, convergence will become more operational and more measurable.

Zero trust is expanding into OT and facilities, and critical manufacturing sectors are facing greater scrutiny from boards, insurers, and regulators. Insurance underwriting expects documented security controls, consistent evidence capture, and repeatable response procedures.

Physical security systems continue to consolidate onto enterprise networks, which increases the importance of device posture, segmentation, and logging. As a result, platforms that standardize the human and facility layers and make them usable for investigations and response become a core input to resilience and safety outcomes rather than a side system.

Black expects carriers to keep shifting toward evidence-based underwriting, with tighter terms or tougher renewals for contractors that cannot demonstrate repeatable operating controls.
In that environment, standardized frontline reporting becomes both a resilience input and a financial lever: it supports claims defense with GPS-verified activity logs and photo-backed inspections, and it strengthens renewal conversations by making the operating model auditable across sites.

How Trackforce Can Help

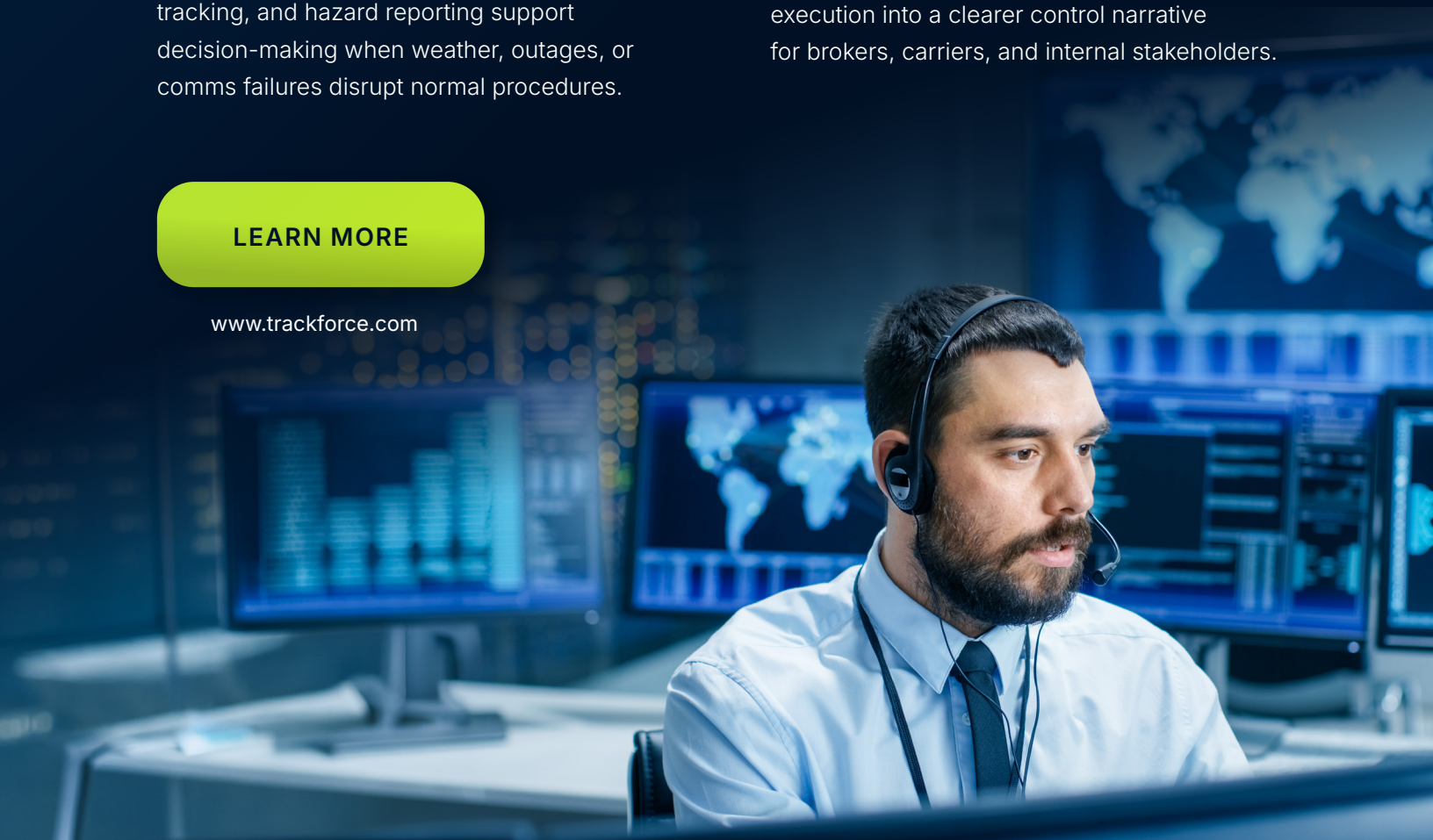
Manufacturing security teams need consistent execution at the facility level and documentation that holds up when operations are disrupted, incidents occur, or risk teams ask for proof.

Where Trackforce creates leverage:

- **Standardized frontline reporting across sites:** Consistent activity logs, patrol reporting, and incident capture reduce handoff friction between shifts and facilities and make timelines easier to reconstruct.
- **Faster investigations with stronger defensibility:** Time-stamped records, location verification, and photo-backed inspections accelerate fact-finding and strengthen duty-of-care documentation.
- **Operational continuity during disruptions:** Real-time workforce status, shift compliance tracking, and hazard reporting support decision-making when weather, outages, or comms failures disrupt normal procedures.
- **Identity discipline for the extended workforce:** Visitor and contractor workflows, credential oversight, and offboarding evidence reduce gaps created by third parties and frequent role changes.
- **Fits into existing enterprise workflows:** Structured reporting can be routed into security, compliance, and case management processes to improve correlation and reduce reliance on informal channels.
- **Supports renewal and risk conversations:** Audit-ready reporting helps translate day-to-day execution into a clearer control narrative for brokers, carriers, and internal stakeholders.

LEARN MORE

www.trackforce.com



The Global Standard in Physical Security Operations

trackforce®

www.trackforce.com

hello@trackforce.com

(USA) +1(888) 454-5606
(CAN) +1(514) 312-2870