KATALYST

DIGITAL OPERATIONS PARTNER

MANUFACTURING EDITION

2026 Katalyst Cybersecurity Executive Report

Securing Your Digital Backbone

How Manufacturers Are Securing Production, Reducing Disruption Risk, and Strengthening Their Digital Backbone in 2026

In manufacturing, cybersecurity is no longer an IT issue. It is an operational issue. A ransomware event does not just lock files. It stops production lines, disrupts shipping, breaks customer commitments, and creates measurable revenue loss. The manufacturers building resilient digital backbones are protecting production continuity and strengthening their competitive position in 2026.

This report is your benchmark. Your baseline. Your starting point.

#1
most-attacked industry — 4 years running

$125k/hr
avg cost of manufacturing downtime

70%+
of manufacturers report OT visibility gaps

OT+IT
convergence expanding attack surface

EXECUTIVE LETTER

A Message From Our CEO

Something has shifted in the conversations I have with manufacturing leaders. They are no longer asking whether cybersecurity matters to production. They are asking why it feels so hard to get under control, and what it will take to get ahead of it.

- **Downtime now stops production, not just email**
- **Boards are asking different questions**
- **OT and IT convergence is expanding the attack surface**
- **Modernization and security are colliding**
- **Supply-chain and vendor sprawl is compounding exposure**
- **Internal bandwidth has reached its limit**

The manufacturers that solve this in 2026 carry a durable advantage forward. They protect production continuity, pass audits and insurance renewals with less friction, and keep their commitments to customers. The ones that don't keep paying in downtime, missed shipments, broken contracts, and competitive ground they cannot easily recover.

Luke Johnson
CEO, Katalyst
Digital Operations Partner

The conversation in every manufacturing boardroom has changed. Technology risk is no longer a footnote in the annual report. It is a standing agenda item in operations and risk reviews across organizations of every size, because when systems go down, production is what stops.

> *"The Digital Backbone must be intentional. It cannot be inherited, assembled by accident, or managed by whoever has time."*

What does that mean in practice? It means the infrastructure your business depends on, the plant network, the ERP and production systems, the OT environment on the floor, and the Microsoft 365 platform your teams work in every day, needs to be owned, operated, and improved with the same discipline you apply to production itself.

Security is a discipline, not a purchase.

The manufacturers pulling ahead are not those with the most tools. They have the clearest accountability and the most consistent execution across every site.

Compliance is a floor, not a ceiling.

Insurers, customers, and auditors are raising expectations faster than most manufacturers are raising their posture. Documented, tested controls are the baseline, not the goal.

The co-managed model is how this gets solved.

Manufacturers cannot hire their way to security maturity. Embedded partnership with shared accountability is the answer.

THE EXECUTIVE SHIFT IN 2026

Six Forces Reshaping Technology Leadership

Manufacturers are balancing growing cybersecurity threats, operational resilience, workforce modernization, and increasingly connected production environments. These are six forces reshaping technology leadership in 2026.

01

Security Leadership Has Changed

Cybersecurity is now an operational and executive responsibility. Technology leaders are expected to protect production, manage enterprise risk, and build resilience across both IT and operational technology environments.

02

Supply Chain Risk Is Increasing

Manufacturers depend on suppliers, logistics partners, equipment vendors, and cloud providers to keep operations running. Managing third-party risk has become essential to maintaining production continuity and protecting critical systems.

03

Connected Operations Are Expanding Risk

Connected production equipment, Industrial IoT, cloud platforms, ERP systems, and remote vendor access continue to expand the manufacturing technology ecosystem. Every new connection introduces additional operational and cybersecurity risk.

04

Technology Priorities Continue to Expand

Technology teams are balancing cybersecurity, production uptime, infrastructure modernization, AI adoption, and operational efficiency while supporting both IT and OT environments. Strategic priorities increasingly compete for the same resources.

05

Operational Resilience Is Now a Competitive Advantage

Downtime, supply chain disruptions, and cyber incidents directly affect production schedules, customer commitments, and revenue. Operational resilience has become a key business differentiator.

06

Digital Manufacturing Is Expanding the Attack Surface

Smart factories, connected production lines, cloud adoption, remote access, and AI-enabled operations continue to expand the attack surface. Security should be built into modernization initiatives from the beginning.

When Production Stops, Revenue Stops in Manufacturing Operations

- Production continuity and uptime
- OT + IT convergence risk
- Supply chain and vendor exposure
- Remote access governance
- Cyber insurance and compliance

In 2026, cybersecurity is no longer a back-office IT concern for manufacturers. It is an operational risk that belongs on the plant floor, in the boardroom, and in every conversation about production continuity and competitive resilience.

83% increased remote access to production environments

58% of industrial environments rely on legacy systems

24/7 production uptime expectations across operations

The manufacturers that move from reactive incident response to intentional digital backbone management are gaining something their competitors cannot easily replicate:

Confidence.

78%
of manufacturers experienced ransomware impacts

$5.58M
avg cost of an industrial cyber incident

54%
of plants lack OT asset visibility

46%
of manufacturers cite a cyberattack on a supplier or vendor as a top operational risk

OT + IT Convergence Is Expanding the Attack Surface.

68%
increased remote plant access

20+ days
avg manufacturing recovery timeline

42%
of industrial sites lack network segmentation

4X
increase in connected industrial devices

3–10+
sites the typical mid-market manufacturer operates, each one expanding the attack surface

The challenge is twofold: modernizing fast enough to close legacy gaps, and securing that modernization as you go.

Manufacturing is among the top 3 most targeted industries globally

Production data, IP, customer contracts, and ERP systems all carry premium value for attackers. Ransomware groups specifically target manufacturers because downtime creates immediate pressure to pay.

Flat network architectures make lateral movement easy for attackers

Without segmentation between corporate IT and plant floor systems, an attacker who gains initial access has a clear path to production. Network architecture is a security decision.

OT and IT convergence has fundamentally changed the risk profile

Connected production equipment, industrial IoT, and remote plant access have erased the old air gap. A credential compromise that once only threatened email now has a path to production systems.

Remote access to production systems is now a primary attack vector

Vendors, engineers, and plant managers accessing systems remotely without enforced MFA is one of the most commonly exploited entry points in manufacturing incidents.

Supply chain dependencies create cascading exposure

A breach at a supplier, distributor, or logistics partner can disrupt your operations even if your own systems are clean. Third-party risk in manufacturing is operational risk.

20+ days of downtime is not a statistic. It is measurable revenue loss.

For a mid-size manufacturer, 20 days offline means missed shipments, broken contracts, idle facilities, and customer relationships that take years to rebuild.

Identity Is the New Perimeter

Identity

68% increased remote access to production systems

Remote access to production systems, vendor logins to plant floor equipment, and engineering credentials with broad system access are the primary identity risks in manufacturing environments. Without enforced MFA and access governance, a single compromised credential can provide an attacker with direct access to production systems. Cyber insurance underwriters are now explicitly requiring MFA documentation for manufacturing policy renewals. Organizations that cannot demonstrate enforcement are facing denials and exclusions. Access rights reviews, vendor credential governance, and conditional access policies are no longer optional. They are the baseline that insurers, customers, and auditors now expect.

Email

$50B+ of attacks target supply chain operations

Engineering teams, procurement departments, vendor contacts, and executive leadership are all high-value phishing targets in manufacturing. Business email compromise leading to fraudulent wire transfers and vendor payment redirection is a leading loss event. AI-driven phishing has dramatically increased sophistication. Attackers now craft messages referencing specific production orders, supplier names, and internal processes, making them nearly indistinguishable from legitimate communications. Email security without continuous tuning leaves significant gaps. A configuration set during initial deployment does not reflect the current threat environment.

60%+ of breaches involve compromised credentials

MFA now required by most cyber insurers

75% of attacks originate through email or identity

30% of manufacturing breaches begin with stolen or compromised credentials

Recovery Is a Strategic Function

Many manufacturing environments reviewed had never conducted a documented restore test, even those with active backup systems running daily.

20+

days average time to restore production after a ransomware event

In manufacturing, backup failure is a production failure. ERP systems, production configuration data, engineering documentation, and file shares are the operational core of a manufacturing business. When ransomware hits and backups are unavailable or untested, the path to recovery is measured in weeks, not hours. That gap is exactly where attackers apply pressure to force payment.

Backups alone are not protection. Tested, segmented, immutable backups are.

The backup job completing successfully is not the same as the backup restoring successfully within your required recovery window. Quarterly restore tests, documented and reviewed by operations leadership, are the standard cyber insurers and auditors now require.

$5+ million

average total cost of a manufacturing cyber incident

RTO and RPO must reflect production reality, not policy aspirations.

A recovery time objective that says '4 hours' but has never been tested against your actual ERP and production systems is a false assumption. If your recovery objectives have not been validated in the past 12 months, you do not know if they are achievable.

Complexity Increases Cost. Katalyst Reduces It.

> *"Katalyst is an accelerator to my team. I don't have to staff every new skill set internally—I can rely on Katalyst to advise and execute when needed. They enable my team to move faster."*
>
> -- VP & Chief Information Officer at The AZEK Company

1

No Unified Visibility

Different firewall vendors across facilities, separate monitoring tools, inconsistent endpoint protection. No single view of what is exposed across the organization.

When a security event occurs, IT teams are correlating data from five different dashboards and calling individual site contacts. That delay is exactly what attackers rely on.

How Katalyst Helps:

Centralized monitoring and standardized security controls create a unified operational view across facilities, networks, and production environments. Teams respond faster because visibility no longer stops at individual sites.

2

Configuration Drift

What was configured correctly at one site gets changed, overwritten, or ignored at another. Multi-site environments amplify inconsistency over time.

Configuration drift is the silent accumulation of security gaps. It rarely causes an obvious failure until an attacker exploits the gap that nobody knew had opened.

How Katalyst Helps:

Standardized configurations, continuous validation, and centralized oversight reduce inconsistency across plants and remote facilities. Security posture becomes measurable, repeatable, and easier to maintain at scale.

3

OT Blind Spots

Plant floor systems, industrial IoT, and production equipment are often outside the scope of corporate security monitoring, even when they are network-connected.

The most dangerous attack surface in manufacturing is often the one nobody is watching. Connected production systems without monitoring are not protected. They are assumed to be safe.

How Katalyst Helps:

Integrated OT and IT monitoring extends visibility to production systems, industrial IoT, and connected equipment without disrupting operations. Manufacturers gain the ability to detect threats before they impact production continuity.

48%
lack visibility into connected OT assets

3–5
security platforms common across plants

62%
operate hybrid OT/IT environments

AI Is Not a Future Problem. It Is a Present Multiplier.

AI-Generated Phishing

AI-generated phishing campaigns are becoming more convincing, personalized, and difficult to detect across manufacturing operations.

Attackers use AI to mimic executives, engineering teams, procurement staff, trusted suppliers, and operational communications. Technical controls remain essential, but ongoing security awareness training is becoming equally important.

AI-Powered Vulnerability Discovery

AI is dramatically reducing the time between finding vulnerabilities and exploiting them.

New AI-powered vulnerability discovery tools can identify weaknesses and generate exploit paths in hours instead of weeks. Manufacturers relying on periodic scans or delayed remediation are increasingly at risk of falling behind.

Supply Chain Impersonation

AI-generated impersonation is making supplier fraud and payment scams more convincing than ever.

Fraudsters are using AI to impersonate suppliers, logistics partners, and internal stakeholders to manipulate payment approvals, banking changes, and procurement workflows. Verification procedures and identity controls are becoming critical safeguards.

AI isn't just creating new threats. It's dramatically accelerating how quickly attackers can exploit existing ones.

Recent demonstrations from AI-powered vulnerability discovery platforms such as Mythos show that vulnerability discovery and exploit development can now happen in hours instead of weeks. Manufacturers need an ongoing vulnerability management program to continuously identify, prioritize, and remediate risk before attackers can take advantage.

The Risk to Manufacturers Is Immediate

AI is increasing the speed, scale, and sophistication of attacks targeting manufacturers. Organizations are seeing more AI-generated phishing, supplier impersonation, ransomware, intellectual property theft, and AI-powered vulnerability discovery. At the same time, employees are increasingly using public AI tools without understanding the security implications, creating new avenues for proprietary information and operational data to be exposed.

Manufacturers that combine security awareness training, secure access controls, behavioral monitoring, centralized visibility, and a mature vulnerability management program are significantly better positioned to reduce risk before attacks disrupt production or expose critical intellectual property.

Security Awareness Training

Build a security-aware culture through ongoing phishing simulations, end-user education, and reporting workflows that help employees recognize evolving AI-powered attacks targeting production, engineering, and procurement teams.

Secure Access (SASE)

Protect proprietary information by applying consistent access policies, web filtering, and data controls across users, devices, cloud applications, and remote access. This also helps reduce risk from Shadow AI and unintended data exposure.

Managed Security Services

Behavioral monitoring, anomaly detection, and centralized visibility across identity, email, endpoints, production systems, and operational technology (OT) enable faster detection and response before incidents disrupt operations.

Vulnerability Management

Continuously identify, prioritize, and remediate vulnerabilities across IT and operational technology environments to reduce the growing window of exposure created by AI-powered discovery tools.

The Accountability Gap Is Not Tool Access. It Is Operational Discipline.

High Performers

- **Standardize firewall and network architecture across all sites**
  Consistent configuration eliminates the gaps that form between differently managed facilities.
- **Segment OT from IT environments with enforced boundaries**
  Network segmentation limits lateral movement and protects plant floor systems from corporate network compromises.
- **Enforce MFA across all remote access and vendor connections**
  Not just enabled, but enforced, monitored, and reviewed against the full list of remote access paths quarterly.
- **Conduct documented quarterly backup and restore testing**
  Restore tests are scheduled, executed, and results reviewed by operations leadership, not filed and forgotten.
- **Implement 24/7 centralized monitoring across all sites**
  A single view of all facilities with defined escalation paths and documented response procedures.

Lower Performers

- **Maintain site-by-site configurations without standardization**
  Each facility becomes its own security island. Gaps accumulate silently between sites.
- **Rely on reactive incident response without monitoring**
  The first sign of a breach is production disruption, not an alert. By then, damage is done.
- **Lack visibility into OT-connected systems**
  Plant floor equipment on the network without monitoring is unprotected by any meaningful measure.
- **Operate without structured resilience reviews**
  Backups have not been tested. Incident response has not been practiced. Recovery time is unknown.
- **No structured reporting to operations or executive leadership**
  Leadership cannot make informed capital decisions about technology risk they cannot see or measure.

Moving from Disruption Risk to Operational Continuity

FROM

Site-by-site configurations

Manufacturing facilities often evolve independently over time, creating inconsistent security controls, network standards, and operational visibility across plants, warehouses, and remote sites.

TO

Standardized architecture

Security posture should not vary by facility. A unified backbone means every site operates under consistent, auditable controls regardless of size or location.

FROM

Reactive incident response

Security and operational teams frequently respond after production disruptions occur instead of identifying threats early enough to prevent downtime, operational delays, and plant-wide impact.

TO

Proactive monitoring

Manufacturers cannot afford to learn about breaches when production stops. 24/7 monitoring means threats are identified before they reach the plant floor.

FROM

Vendor sprawl

Disconnected vendors managing networking, OT systems, cybersecurity, remote access, and infrastructure create overlapping tools, inconsistent accountability, and growing operational complexity.

TO

Strategic consolidation

Multiple vendors creating inconsistent configurations wastes budget and hides gaps. Consolidation improves visibility, reduces cost, and strengthens insurance documentation.

FROM

Isolated plant systems

Production environments were historically designed for uptime and isolation, not visibility and integration. As OT and IT converge, disconnected systems create blind spots that increase operational and cybersecurity risk.

TO

Segmented, monitored integration

OT and IT convergence is not going backward. The answer is not isolation. It is segmentation with monitoring that gives you visibility without disrupting production.

Production resilience is not accidental. It is designed.

Resilience Is Built Intentionally

High-performing manufacturers treat their digital environment as operational infrastructure, not overhead. A resilient manufacturing digital backbone is standardized across sites, designed with OT/IT segmentation in mind, and continuously monitored.

01 CONNECT

Hybrid infrastructure, cloud platforms, and network connectivity managed as one cohesive environment. From on premises infrastructure and Azure to SD WAN, branch offices, and remote access, Katalyst standardizes, monitors, and optimizes how everything connects. Katalyst is accountable for keeping the digital backbone connected, stable, and operational end to end.

- SD-WAN & Networking
- Cloud Connectivity
- Branch & Remote Access
- Managed Infrastructure

02 PROTECT

Security is not a standalone product. It is an operational discipline. Katalyst aligns identity controls, endpoint protection, email security, compliance requirements, monitoring, and incident response into one managed security posture. Katalyst is accountable for continuously reducing risk, validating controls, and strengthening resilience across the environment.

- Identity & MFA
- EDR & Endpoint
- Email Security
- MDR
- Cybersecurity
- Compliance
- MSSP
- SIEM

03 OPERATE

24/7/365 operational management backed by strategic guidance and measurable accountability. Katalyst provides continuous monitoring, help desk support, Microsoft 365 management, backup validation, security oversight, and operational reviews focused on ongoing improvement. Katalyst is accountable for helping organizations operate more efficiently, recover faster, and continuously strengthen their digital backbone over time.

- Help Desk
- Backup & DR
- Microsoft 365
- Advisory & QBRs
- vCIO
- Managed Security
- Managed Infrastructure

The backbone is not about adding tools. It is about operating them intentionally.

A Practical Roadmap for 2026

1 Immediate
0-90 Days

- **Review remote access and vendor MFA enforcement**

  Audit every remote access path into your environment, including VPN, vendor portals, and plant system access. Enforce MFA on all of them. Gaps here are the fastest path to a production incident.

- **Validate network segmentation between OT and IT**

  Confirm that your plant floor systems and production equipment are properly segmented from corporate IT. If you have never documented or tested this boundary, that is the first thing to address.

- **Confirm backup testing documentation**

  Pull the last restore test record covering your ERP and production systems. If it is more than 90 days old or does not exist, schedule one immediately.

2 Mid-Term
3-6 Months

- **Standardize firewall and security stack across facilities**

  Eliminate the patchwork of site-specific tools. A consistent security stack across all facilities makes monitoring possible, reduces vendor management complexity, and closes configuration gaps.

- **Implement centralized monitoring**

  Establish a single view of all sites and production environments. Every alert should have an owner, a response procedure, and an escalation path to operations leadership.

- **Formalize incident response procedures**

  Document who does what when an incident occurs across IT, operations, legal and executive leadership. Walk through it before you need it.

3 Long-Term
6-12 Months

- **Establish digital backbone governance across sites**

  Define clear ownership for Connect, Protect, and Operate across your organization. Document accountability, performance metrics, and how security posture is reported to leadership.

- **Conduct resilience testing simulations**

  Tabletop exercises and backup restore tests should be on the annual calendar, mandatory, documented, and reviewed by operations and executive leadership.

- **Align IT strategy with production growth initiatives**

  Every new facility, production line, or automation investment creates new infrastructure. Security architecture decisions made at the start are far cheaper than remediating them later.

Ready to strengthen your digital backbone? Schedule a conversation with Katalyst.

KATALYST

DIGITAL OPERATIONS PARTNER

Your Digital Backbone. Owned. Operated. Continuously Improved.

katalystng.com
704-790-4440
Charlotte, NC | Spartanburg, SC

Assess.
Benchmark your environment across Connect, Protect, and Operate.

Transform.
Build and execute a practical, prioritized roadmap.

Manage.
Ongoing ownership, visibility, and continuous improvement — 24/7/365.

> *"Cybersecurity is a race, a marathon you have to keep running. [Working with Katalyst] is like having a team that's going to help you win this marathon."*
>
> **IT Director · NC Food Manufacturer**

> *"What I appreciate most is trust. I know Katalyst is invested in our journey, and that makes them more than a vendor -- they are a partner I can count on."*
>
> **Michelle Kasson · VP & CIO, The AZEK Company**

> *"Katalyst is there when you need them and things get handled. The team knows the environment like the back of their hand. When you find a company that has the expertise and the ability to provide seamless, continuum of service you keep that."*
>
> **Nancy Warren · IT Director, HVO**

SOURCES & REFERENCES

1 Manufacturing Cybersecurity Research 2025-2026

2 Ransomware & Data Exfiltration Reports 2025

3 Identity Compromise & Phishing Research 2025

4 OT/IT Convergence Risk Studies 2025

5 Supply Chain Cyber Risk Analysis 2025

6 Cyber Insurance Underwriting for Manufacturing 2025

7 IBM Cost of a Data Breach -- Industry Analysis 2024

8 AI Phishing & Industrial Threat Analysis 2025

9 Manufacturing Ransomware Downtime Studies 2025

This report is produced by Katalyst for informational purposes. Statistics sourced from publicly available industry research. Verify against primary sources before formal reporting.

Digital Backbone Assessment
Benchmark your full environment across Connect, Protect, and Operate.

30-Day Satisfaction Guarantee
If we are not delivering, we make it right or we refund you.

Start the Conversation
katalystng.com · 704-790-4440
Charlotte, NC | Spartanburg, SC