octoplant

EFA AUTOMAZIONE | Proud member of RELATECH

REPORT

THE EUROPEAN OT SECURITY LANDSCAPE

An Octoplant Analysis, Based on Exclusive Statista Research, Exploring International Trends, Technologies, and Strategic Directions in OT Security

TABLE OF CONTENTS

FOREWORD 4

EXECUTIVE SUMMARY 5

CHAPTER I: OT ENVIRONMENT
The Operational Technology Landscape
CHAPTER II: DISRUPTIONS IN OT
Outages and Downtime in OT Environments 9

CHAPTER III: OT SECURITY
Securing Industrial Systems 20

CHAPTER IV: OT DEVELOPMENT
Investment and Innovation in OT 31

47

FOREWORD

The industriallandscape standsat an unprecedented crossroads. As we advance deeper into the digital age, operational technology (OT) systems that once operated in isolated environments now find themselves at the heart of a connected, data-driven industrial ecosystem. This transformation brings extraordinary opportunities for efficiency, innovation, and competitive advantage—but also introduces new vulnerabilities and challenges that demand urgent attention.

The year 2024 proved to be a watershed moment for industrial cybersecurity and operational resilience. With over 83% of OT leaders experiencing security breaches and a 146% increase in cyberattacks leading to physical operational disruptions, the stakes have never been higher. Yet paradoxically, this same period witnessed remarkable advances in predictive analytics, artificial intelligence integration, and autonomous systems that promise to revolutionize industrial production.

This comprehensive report examines the current state of operational technology across global industrial enterprises, revealing both the achievements and critical gaps that will determine which organizations thrive in the increasingly digital industrial landscape. Through extensive research encompassing organizations of all sizes and sectors, we present not merely data, but strategic insights that can guide decision-makers through the complex challenges of digital transformation whilst maintaining operational excellence and security resilience.

The findings contained within these pages should serve as both a wake-up call and a roadmap for industrial leaders. The organizations that master the convergence of operational excellence with technological innovation will define the future of industry. Those that fail to act on these insights risk not merely competitive disadvantage, but potential obsolescence in an economy where technological capability increasingly determines market leadership.

The survey was conducted by Statista among 187 respondents representing industrial organizations across several European countries. Participants came from Austria (24%), Italy (27%), Spain (27%), Finland (8%), Denmark (7%), Norway (5%), and Sweden (2%).

Respondents worked in a variety of industries, with the largest shares from manufacturing and industrial sectors (34%), chemicals, pharmaceuticals, and life sciences (28%), energy, utilities, and natural resources (17%), and food and beverage (10%). Other sectors such as construction, IT and digital services, entertainment, and consumer goods were also represented.

Companies varied in size, with 54% of respondents working for organizations employing 300–499 people, 12% in companies with 500–999 employees, 19% in enterprises with 1,000–5,000 employees, and 16% in larger firms with over 5,000 employees. Regarding organizational roles, 15% of respondents held top management or C-level positions, 23% were division or department heads, 9% served as team leads, 32% were employees without managerial responsibilities, and 22% were domain experts with specialized knowledge.

In terms of functional specialization, over half (53%) identified as cybersecurity analysts or consultants, 14% as IT managers, 13% as engineers or technicians, 12% as OT managers, and 3% as automation managers. Among senior management, 78% held the title of Chief Technology Officer (CTO), and 22% were Chief Information Security Officers (CISO).

This diverse respondent profile offers insights into the operational and cybersecurity challenges faced by industrial organizations of varying sizes, sectors, and geographical locations.

EXECUTIVE SUMMARY

The Digital Maturity Paradox: Promise vs. Reality

Contemporary industry faces a stark contradiction at the heart of its digital transformation journey. Whilst leaders proclaim an Industry 4.0 revolution, our research reveals that only 33% of organizations maintain fully automated, centralized OT asset inventories. This means that 67% of enterprises still operate through hybrid models combining advanced technologies with time-consuming manual processes—a reality that creates significant operational vulnerabili- ties and competitive disadvantages.

Key Findings: The State of Industrial Technology

Operational Excellence Drives Digital Success Our research establishes a powerful correlation between operational stability and technological advancement. Organizations with very stable OT environments achieve 46% full automation compared to just 10-13% among unstable environments. This finding fundamentally challenges the assumption that technology adoption leads to stability—instead suggesting that operational excellence provides the foundation for successful digital transformation.

The Scale Advantage: Size Determines Digital Capability

- **Large enterprises (5,000+ employees):** 72% achieve full automation
- **Mid-sized companies (1,000-5,000 employees):** 60% full automation
- **Small enterprises (300-499 employees):** Only 12% full automation

This dramatic scaling effect reveals that digital transformation benefits compound with organizational size, potentially creating competitive fragmentation across industry sectors.

Universal Technology Adoption Masks Implementation Challenges

While**98%of organizationsdeploy corecontrolsystems** (SCADA,DCS, PLC),the management sophistication varies dramatically. Real-time vulnerability monitoring is practiced by only **47% of organizations**, and structured patch management drops to **75% in stable environments**—revealing dangerous complacency where it's least expected.

THE DISRUPTION REALITY: HIDDEN COSTS AND PERCEPTION GAPS

Downtime Dominates Industrial Challenges

62% of organizations experienced system downtime and equipment failures over the past three years. However, our findings reveal alarming perception gaps:

- **88% of technical specialists** recognize downtime as a primary concern
- **Only 41% of strategic decision-makers** acknowledge the same issue

This disconnect between operational reality and executive awareness represents a critical risk factor for strategic planning and investment decisions.

Small Firms Face Disproportionate Exposure

68% of small organizations (300-499 employees) experience significant downtime compared to **44% of mid-sized enterprises (1,000-5,000 employees)**. This vulnerability stems from legacy infrastructure dependencies, limited redundancy capabilities, and resource constraints in specialized OT maintenance.

CYBERSECURITY: HIGH CONFIDENCE, HARSH REALITY

The Preparedness Paradox

Despite **90% of organizations expressing confidence** in their cybersecurity preparedness, the incident reality tells a different story:

- **71% experienced data breaches or unauthorized access** in the past year
- **52% encountered malware infections**
- **43% faced insider threat incidents**

Mid-Sized Enterprise Vulnerability

Companies employing 500-999 people face a perfect storm of cybersecurity challenges:

- **100% reported unauthorized access incidents**
- **Only 68% plan to invest in OT-specific cybersecurity improvements**

This creates a dangerous risk-investment paradox where the most vulnerable segment shows the lowest intent for protective investments.

FUTURE INVESTMENT PRIORITIES: INNOVATION WITH IMPLEMENTATION GAPS

Predictive Technologies Achieve Universal Appeal

88% of organizations plan to implement predictive maintenance and real-time analytics, establishing these as baseline operational expectations rather than competitive advantages.

Autonomous Systems Create Strategic Divides

81% express intent for autonomous production lines, but a dramatic **36-point gap** exists between C-level enthusiasm (96%) and middle management support (60%)—representing one of the most significant alignment challenges in our research.

AI Integration Gains Mainstream Acceptance

77% plan AI and machine learning integration, with particularly high enthusiasm among companies with unstable OT environments (91%), suggesting operational challenges drive innovative technology adoption.

The Middle Management Challenge: A Critical Implementation Barrier

Across every major technology category—cybersecurity (67%), IT-OT convergence (67%), and AI/ML (67%)—**division/department heads consistently show lower engagement** than both executive leadership and technical teams. This persistent pattern represents a critical bottleneck in strategic implementation that could undermine transformation initiatives across the industrial sector.

THE PATH FORWARD: CONVERGENCE AS COMPETITIVE ADVANTAGE

Downtime Dominates Industrial Challenges

Our research demonstrates that future industrial success belongs to organizations that achieve convergence between **operational excellence and technological innovation**. This convergence requires:

1. **Strategic alignment** across all organizational levels
2. **Phased implementation** strategies that build capability progressively
3. **Ecosystem thinking** that recognizes interdependence across supply chains
4. **Adaptive resilience** enabling rapid response to technological and market changes

The organizations that master this convergence will not merely survive the digital transformation - they will define the future of industrial competition. Those that fail to address the fundamental challenges revealed in this research risk marginalization in an economy where technological capability increasingly determines competitive advantage.

CHAPTER I

THE OT ENVIRONMENT LANDSCAPE

Analysis of Industrial Digital Transformation Fundamentals

- Currentstateof OT infrastructure and digitalmaturity
- Asset management automation and centralization trends
- Technology adoption patterns across organizational scales
- Correlation between operational stability and digital advancement

INTRODUCTION: INDUSTRY AT A CROSSROADS

Modernindustryfindsitselfat a criticaljuncture in itsevolution. Whilst operational technologies (OT) become increasingly integrated with IT ecosystems, organizations must grapple with mounting cybersecurity challenges, asset management complexity, and pressures for process automation. Our research, encompassing a broad spectrum of industrial enterprises, sheds light on the reality of this transformation, revealing both achievements and perilous gaps that may determine the future of entire sectors.

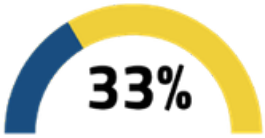
OT ASSET CENTRALIZATION: THE FOUNDATION OF MODERN MANUFACTURING

The Digital Maturity Paradox

One of our study's most striking discoveries is the dramatic disconnect between digital transformation aspirations and operational reality. Whilst industry leaders proclaim an Industry 4.0 revolution, merely 33% of organizations maintain fully automated, centralized OT asset inventories. This means the overwhelming majority – 67% of enterprises – still function within hybrid models, combining advanced tools with time-consuming manual processes.

33%

Organizations with fully automated, centralized OT asset inventories



This isn't merely a technological issue – it's a fundamental strategic challenge. In an era where every minute of downtime can cost tens of thousands of money, and cyber attacks grow increasingly sophisticated, the absence of complete OT asset visibility becomes a luxury industry cannot afford.

Anatomy of the Digital Divide

Analysis of the correlation between organizational size and automation levels reveals profound structural inequalities in technological capabilities:

- **Small and Medium Enterprises: Struggling with Digital Transformation** Companies employing 300-499 workers exhibit the lowest automation maturity levels. Just 12% achieve full OT asset inventory automation, whilst the overwhelming majority – 88% – remain dependent on hybrid automated-manual processes. This state of affairs stems not from lack of awareness, but from real constraints: budgetary, staffing, and organizational limitations.
- **The Tipping Point: Mid-Sized Enterprises** Companies employing 1,000-5,000 workers demonstrate a significant leap in automation sophistication. 60% operate fully automated systems. This threshold appears to represent the critical mass of resources – both financial and organizational – necessary for successful comprehensive OT solution implementation.
- **Corporate Dominance: Full Automation as Standard** Large enterprises employing over 5,001 workers establish the industry benchmark. 72% report fully automated inventory systems, whilst only 20% still rely on hybrid approaches. This statistic not only confirms the correlation between scale and technological capability, but also indicates automation's strategic importance for maintaining competitiveness in the global economy.

Strategic Implications for Industrial Strategy

These data reveal a fundamental truth about contemporary industrial transformation: automation is no longer optional, but a competitive imperative. Organizations failing to keep pace with digital transformation risk not only operational efficiency losses, but also exposure to mounting cybersecurity threats.

OPERATIONAL STABILITY: THE HIDDEN VALUE OF AUTOMATION

Discovering the Stability-Automation Correlation

One of our study's most significant findings is the clear correlation between OT asset inventory automation levels and perceived operational environment stability. This relationship, previously unsuspected by many industry experts, could fundamentally alter how organizations approach automation investments.

Unstable Environments: Lack of Automation as a Barrier

Organizations experiencing mostly stable OT disruptions show alarmingly low inventory automation levels – only 10% maintain fully automated systems. Similarly, 13% of organizations operatingin somewhatunstableOT environmentsreportfull automation.

Stable Environments: Automation as Foundation

In dramatic contrast, organizations operating in very stable environments achieve 46% full inventory automation – nearly five times higher than in unstable environments.

10%
Organizations with full automationin mostly stable environments

13%
Organizations with full automationin somewhat unstable environments

46%
Organizations with full automationin stable environments

Strategic Interpretation

These data suggest that OT asset inventory automation isn't merely a response to existing problems, but a proactive foundation for operational stability. Organizations with fully automated systems gain:

- Asset tracking advantage: Comprehensive visibility of all OT components in real-time
- Incident response acceleration: Faster problem identification and localization
- Comprehensive situational awareness: Better understanding of OT landscape interdependencies

This correlation indicates the need to redefine automation: from costly option to strategic investment in operational stability.

DOMINANT TECHNOLOGIES: THE FOUNDATION OF MODERN INDUSTRY

Near-Universal Adoption of Core Systems

Analysis of technologies deployed across industrial organizations reveals a clear picture of sector priorities. 98% of respondents report implementing both monitoring systems (e.g., SCADA software, DCS) and control systems (e.g., PLC, DCS, RTU). This near-universal penetration confirms these technologies constitute the unassailable foundation of contemporary industrial operations.

Complete Standardization in Key Segments

Particularly significant is achieving 100% adoption of control and monitoring systems among:

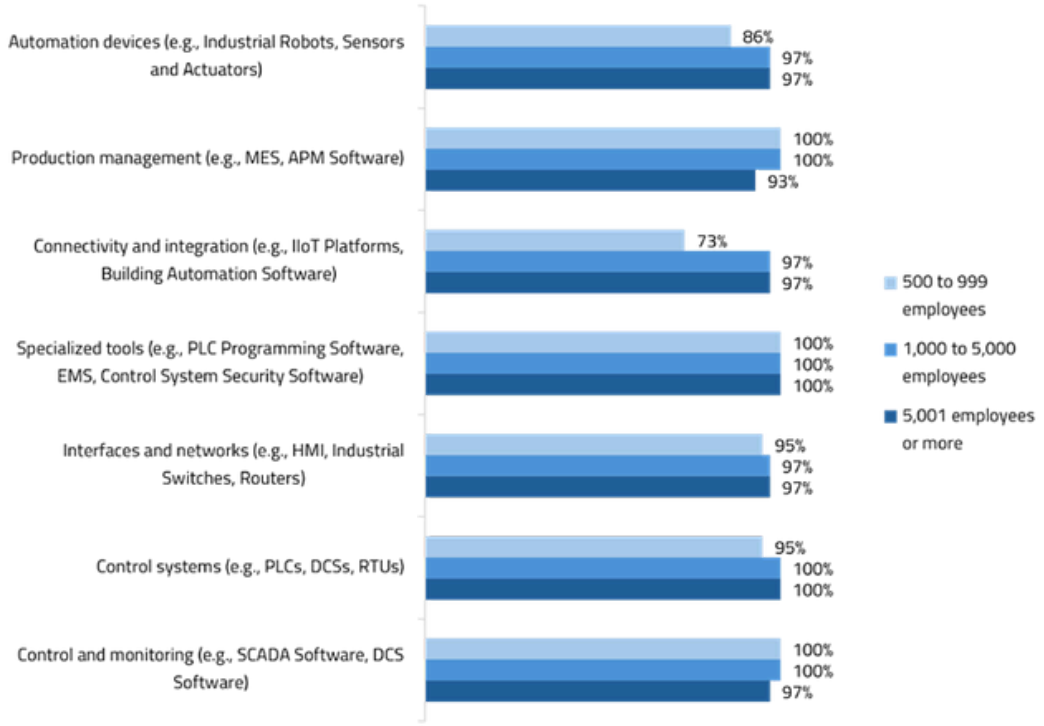
- Companies employing 500-5,000 workers
- Department and team managers
- Organizations operating in very stable OT environments

This complete penetration amongst operational leaders and stable organizations confirms these technologies are not only technically essential, but also strategically prioritized at the highest management levels.

Ecosystem Expansion: Supporting Technologies on the Attack

Whilst core systems achieved near-universal adoption, organizations simultaneously invest intensively in complementary technologies:

- Network infrastructure and interfaces: 97% of organizations implemented interfaces and networks (HMI, industrial switches, routers), indicating growing importance of connectivity and interoperability.
- Specialist tools: 94% of organizations utilize advanced tools (PLC programming software, energy management systems, control system security software), demonstrating the drive towards OT management professionalization.
- Connectivity and integration platforms: 92% of organizations deployed connectivity and integration platforms (IIoT platforms, building automation software), signalling transition towards more integrated ecosystems.



Source: Statista 2025

Strategic Technological Implications

Data confirms SCADA, DCS, and PLC systems remain the technological foundation of contemporary OT deployments. Simultaneously, organizations increasingly integrate advanced tools such as IIoT platforms, HMI systems, and secure network infrastructure. This creates a hybrid technological landscape that enhances connectivity capabilities whilst introducing operational complexity.

OT DEVICES: CONTROL DOMINANCE AND IIOT EXPANSION

Standardization of Core Device Categories

The study reveals exceptional standardization in core OT device categories. 98% of respondents report deploying both control devices (PLC, RTU, DCS) and human-machine interface devices (HMI) in their operational environments. This ubiquitous penetration underscores the fundamental role these systems play in managing industrial processes and visualising control logic.

Universal Deployment in Large Enterprises

100% of respondents from companies employing over 1,000 workers indicated control device deployment. This complete adoption is also reported by:

- Team leaders
- Workers without managerial responsibilities
- Workers with specialized domain knowledge

This universality amongst technical and operational personnel indicates control devices are managed primarily by workers closest to daily operations, confirming their critical importance for real-time functionality.

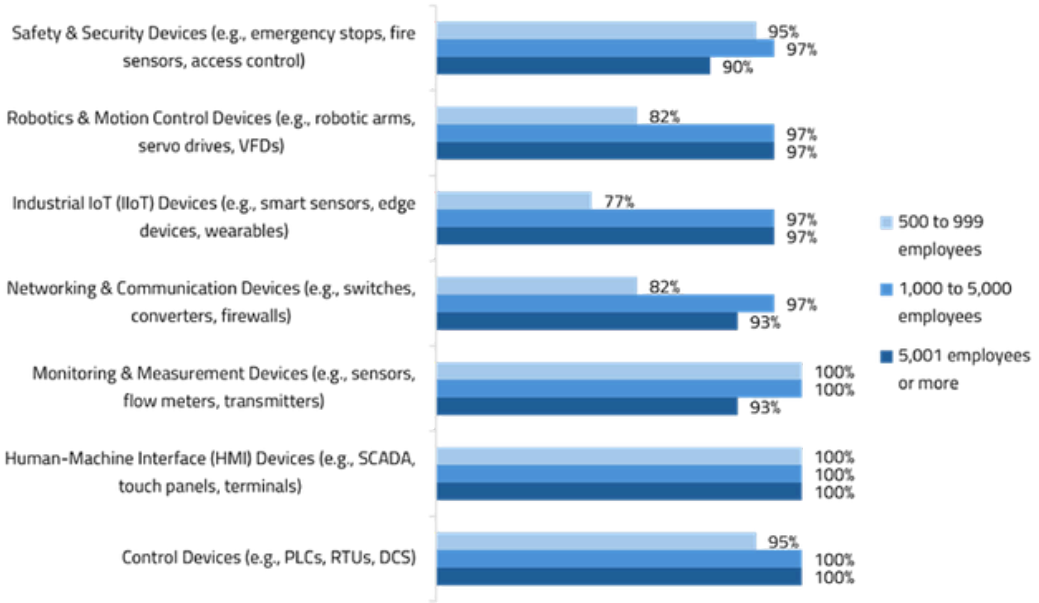
HMI Standardization in Stable Environments

100% of respondents from companies employing over 500 workers report HMI device deployment. Complete adoption is also observed among:

- Team leaders
- Respondents „aware of OT systems but not operationally engaged“
- Organizations operating withverystable OT disruptionlevels

Broad but Incomplete Penetration of Complementary Technologies

- Monitoring and measurement devices: 96% of organizations deployed sensors, flow meters, and transducers, confirming the importance of real-time data collection.
- Network and communication devices: 95% utilize switches, converters, and firewalls, indicating growing importance of secure communication in OT environments.
- Industrial IoT devices: 93% of organizations deployed smart sensors, edge devices, and wearable technologies, signalling transition towards more advanced, connected ecosystems.



Source: Statista 2025

OT DEVICE MANAGEMENT: STRONG FOUNDATIONS, IMPLEMENTATION CHALLENGES

Excellence in Vulnerability Controls

Organizations demonstrate exceptional discipline in fundamental OT device management practices. 98% of all respondents indicate regular vulnerability assessments. This practice was reported by 100% of:

- Senior management/C-level executives
- Department/divisional managers
- Team leaders

Universal adoption among senior management and operational managers demonstrates organizational recognition of cyber threats and commitment to proactive threat identification. This aligns with growing regulatory requirements and the principle that visibility constitutes the first step in industrial risk mitigation.

Version Tracking: Near-Universal Configuration Management Support

97% of respondents report „tracking software/firmware version changes“ on OT devices, indicating high discipline in configuration management and awareness of changes in critical infrastructure.

Patch Management: Widely Practised but Not Fully Institutionalized

92% of respondents report adhering to structured patch management processes. However, this figure drops significantly among organizations with primarily stable OT disruptions, where only 75% report adhering to structured patch management.

This difference reveals a paradox: organizations experiencing operational stability may be less inclined to invest in rigorous patch management processes, potentially exposing themselves to future threats.

TASK FREQUENCY: REAL-TIME MONITORING AS THE NEW STANDARD

Vulnerability Controls: The Real-Time Revolution

47% of all respondents report conducting regular vulnerability assessments in continuous/real-time mode. This adoption is highest among:

- 62% of department/divisional managers
- 56% of respondents engaged in OT system decisions
- 50% of respondents operating in very stable environments

The prioritization of real-time vulnerability scanning by decision-makers and operational leaders underscores growing recognition of cyber-resilience as a continuous state rather than periodic audit.

62%

Division/Department heads

56%

Involved indecisions related to OT systems

50%

Operatinginverystable environments

Version Tracking: Predominantly Monthly, but with Clear Role Differences

50% of all respondents perform software/firmware version change tracking monthly. This includes:

- 70% of respondents from companies employing 500-999 workers
- Only 41% from companies employing over 5,001 workers

Particularly noteworthy:

- 85% of senior management/C-level executives report monthly tracking
- Only 38%ofteamleadersreportsuchfrequency

Backup Management: Weekly Cadence as Standard

43% of respondents state that maintaining OT hardware documentation backups is performed weekly. This includes:

- 56% of senior management/C-level executives
- 57% of those directly responsible for OT systems
- 50% of respondents from very stable environments

OT ENVIRONMENT STABILITY: HIGH PERCEIVED RESILIENCE WITH HEIGHTENED RISK AWARENESS

Prevailing Operational Optimism

A significant majority of respondents – 62% – characterise their OT environments as very stable, with minimal or zero disruptions or problems. Additionally, 26% report environments as „mainly stable, with only sporadic minor disruptions".

Only 12% indicate somewhat unstable environments, with regular disruptions or performance problems.

Strongest Stability Among Larger Enterprises

74% of companies employing 1,000-5,000 workers and 79% of companies employing over 5,001 workers report very stable OT environments. In contrast, only 45% of companies employing 500-999 workers report similar stability.

Significantly, 17% of respondents from the 300-499 worker segment and 18% from the 500-999worker segment indicatesomewhatunstableenvironments.

Stability Perception Varies by Role

55% of department/divisional managers and 56% of senior management/C-level executives describe OT environments as very stable. However, 73% of workers with domain knowledge and 75% of team leaders report the same, showing higher confidence at operational levels.

55%
Division/Department heads

56%
Topmanagement / C-level executives

73%
Domainexperts

75%
Teamleads

In contrast, 24% of those directly responsible for OT systems and 30% of senior management describe environments as somewhat unstable.

STRATEGIC IMPLICATIONS FOR INDUSTRY'S FUTURE

For Small and Medium Enterprises

Data reveals that organizations employing 300-1,000 workers face critical challenges in digital transformation. These enterprises must:

- Prioritize OT asset inventory system automation as a key element of operational stability
- Develop structural patch management processes, particularly in stable environments susceptible to complacency
- Consider strategic partnerships with technology providers to accelerate maturity without proportional capital investments

For Large Corporations

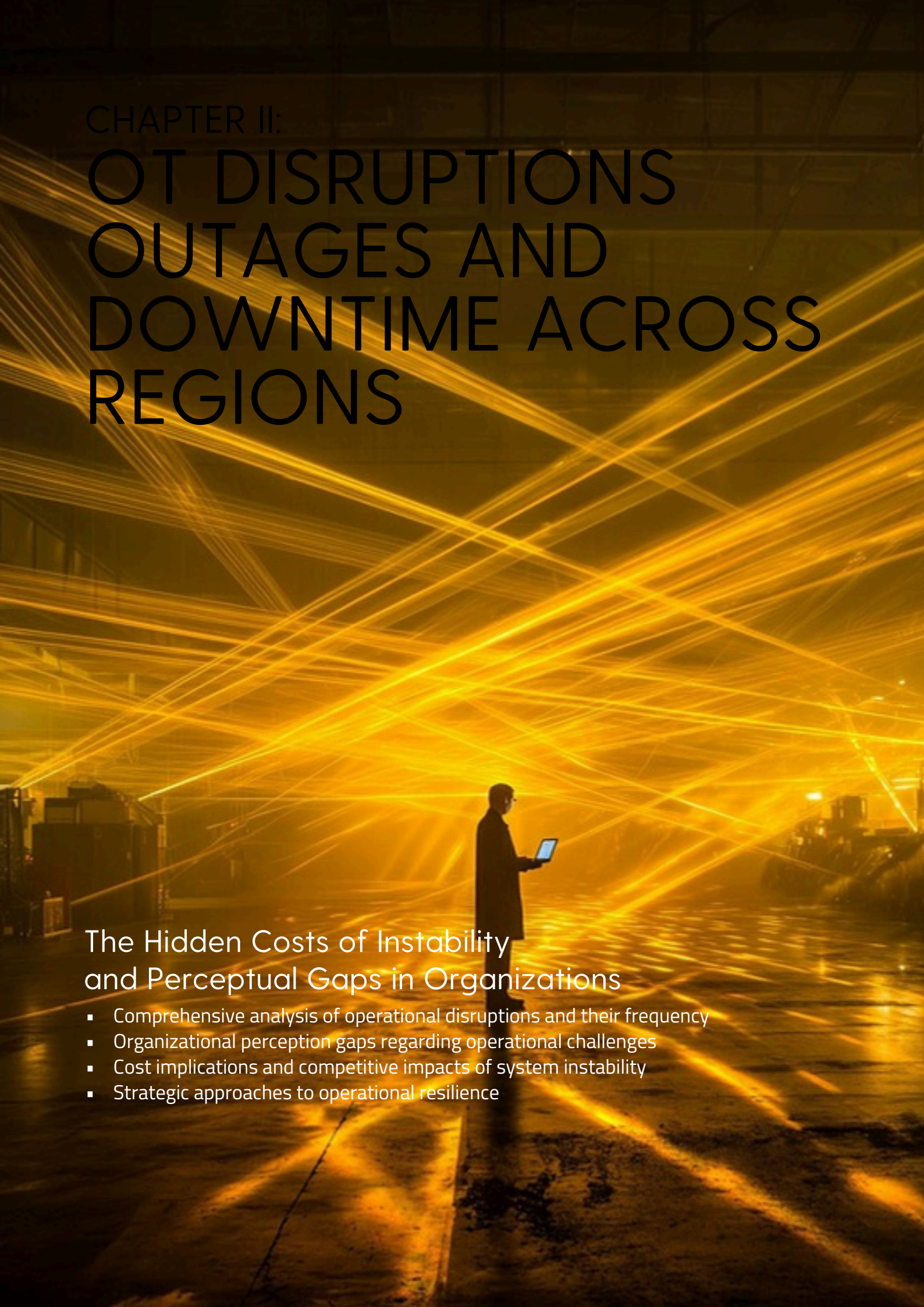
Major enterprises, despite automation advantages, must:

- Leverage their automation advantage to build not only operational but also strategic resilience
- Address the perceived gap between organizational levels in OT risk perception
- Develop support programmes for smaller supply chain partners, recognizing the interconnected nature of modern industrial ecosystems

STRATEGIC IMPLICATIONS FOR INDUSTRY'S FUTURE FOR THE ENTIRE SECTOR

Industry mustrecognize thatOT assetmanagementautomation isn't atechnologicalluxury, but the foundation of operational security and stability. Organizations failing to keep pace with this transformation risk not only a competitive disadvantage, but also exposure to mounting cybersecurity threats in an increasingly connected industrial world.

The future belongs to organizations that can combine operational excellence with cyber resilience, and the key to this combination is fully automated, centralized OT asset management.



CHAPTER II:

OT DISRUPTIONS OUTAGES AND DOWNTIME ACROSS REGIONS

The Hidden Costs of Instability and Perceptual Gaps in Organizations

- Comprehensive analysis of operational disruptions and their frequency
- Organizational perception gaps regarding operational challenges
- Cost implications and competitive impacts of system instability
- Strategic approaches to operational resilience

INTRODUCTION: THE INVISIBLE EPIDEMIC OF INDUSTRIAL DOWNTIME

Whilstthe business worldcelebratesadvancesin industrial automation and digitization, beneath the surface of these achievements lies a troubling reality: operational technology disruptions have become an endemic problem for contemporary organizations. Our research reveals not only the scale of these challenges, but also alarming differences in how their impact is perceived across different organizational levels.

In an era where a single outage can cost the pharmaceutical industry as much as $50,000 per minute, and the automotive sector may lose up to $22,000 for every minute of halted production, understanding the nature and frequency of OT disruptions becomes a matter of competitive survival.

SYSTEM FAILURES: THE MODERN FACTORY'S MOST PERSISTENT ADVERSARY

The Dominance of Downtime as the Primary Threat

System downtime and equipment failures emerge as the most pervasive operational threat in industrial environments, affecting 62% of all respondents over the past three years. This isn't merely a statistic—it's a reflection of a fundamental challenge that shapes the daily reality of contemporary industry.

The Perception Chasm: Technicians vs. Managers

One of the most concerning discoveries in our research is the dramatic difference in how downtime is perceived between different organizational levels. This chasm isn't merely an academic curiosity—it's a symptom of deeper problems in organizational communication that can lead to flawed strategic decisions.

Acute awareness on the front line:

- 88% of those directly responsible for OT systems identify downtime as a primary concern
- 79% of workers aware of OT systems, but not directly involved, also recognize this issue

Limited visibility at strategic level:

- Only 41% of those occasionally interfacing with OT systems
- Merely 42% of those involved in OT-related decision-making processes

Strategic Interpretation: The Cost of Ignorance

This disproportion reveals a critical gap in organizational information flow. Whilst front-line operators maintain acute awareness of failure frequency and impact, executive-level visibility proves insufficient. This can lead to:

- Delayed modernization investments: Management, not fully aware of the problem's scale, may fail to prioritize necessary upgrades
- Inadequate budgeting: Lack of full understanding of downtime costs may lead to underinvestment in preventive solutions
- Flawed risk management strategies: Decisions made without complete operational awareness

ORGANIZATIONAL SIZE: THE PARADOX OF SCALE AND VULNERABILITY

Smaller Firms: Disproportionate Exposure to Downtime

Analysis of the relationship between organizational size and perceived system instability reveals significant asymmetries that may determine the competitiveness of entire market segments.

High exposure in small organizations: 68% of respondents from organizations employing 300-499 people experienced system downtime and equipment failures.

Relative stability in medium enterprises: Only 44% of respondents from companies employing 1,000-5,000 people report similar experiences.

- **Small organizations:**

- **Mid-market:**

- **Large enterprises:**

Anatomy of Small Firm Vulnerability

This disproportion isn't coincidental—it reflects structural challenges faced by smaller organizations:

- Legacy Infrastructure Dependencies: Smaller firms often operate on older infrastructure that is more prone to failure and more difficult to maintain.
- Limited Redundancy Capabilities: Whilst large corporations can afford backup systems and redundant critical paths, smaller organizations often operate without such safeguards.
- Resource Constraints in OT Maintenance: The lack of dedicated OT teams means that system maintenance and monitoring may be irregular or non-specialist.

Strategic Implications for the Industrial Ecosystem

These findings suggest that the small and medium enterprise segment may require targeted support in accelerating OT modernization and implementing reliability engineering initiatives. Otherwise, the growing gap between large and small organizations' capabilities could lead to competitive fragmentation across entire sectors.

PRODUCTION DELAYS: HIDDEN COSTS AND MANAGEMENT BLIND SPOTS

The Second Largest Disruption Category

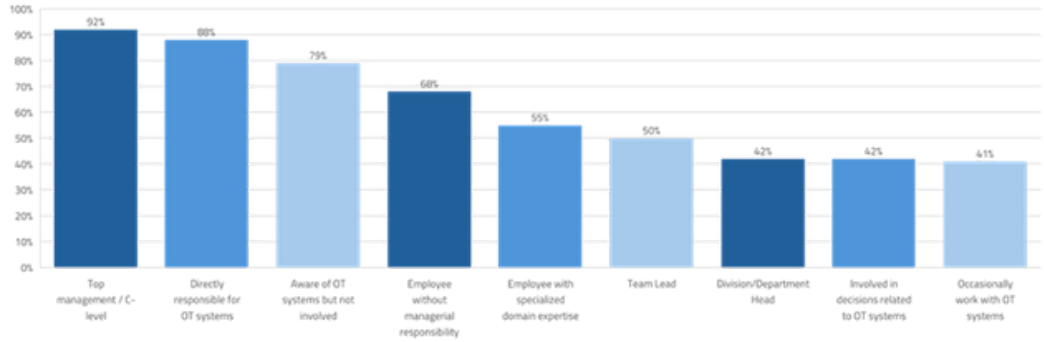
Delays in production or operations were reported by 49% of all respondents, positioning them as the second most prevalent disruption category. However, role-based reporting distribution reveals critical organizational communication failures that could have far-reaching consequences for operational efficiency.

An Alarming Communication Gap

Insufficient management awareness: Only 25% of team leaders acknowledged this issue.

Overwhelming specialist awareness:

- 73% of employees with specialized domain expertise
- 83% of respondents from organizations with somewhat unstable OT environments



Source: Statista 2025

Consequences of the Broken Telephone Effect

This disproportion indicates a breakdown in communication and escalation protocols, where front-line specialists experience significant operational bottlenecks that fail to surface adequately at management levels. This may lead to:

- Inadequate root cause analysis: Without full management awareness, it's difficult to conduct comprehensive problem analysis.
- Delayed implementation of mitigation strategies: Investment decisions in solutions may be made too late or based on incomplete information.
- Team morale erosion: Employees may feel ignored when their reported problems aren't reflected in management actions.

SCALING OF DELAYS: THE BENEFITS OF SIZE

Distribution of Production Delays by Organizational Scale

Analysis of production delays by organizational size reveals an interesting pattern that confirms the theory of economies of scale in operational management:

- 56% of respondents from companies employing 1,000-5,000 people

- 50% of companies employing 300-999 people

- Only 33% of enterprises exceeding 5,000 employees

Organizational Advantages of Large Enterprises

Larger organizations likely benefit from:

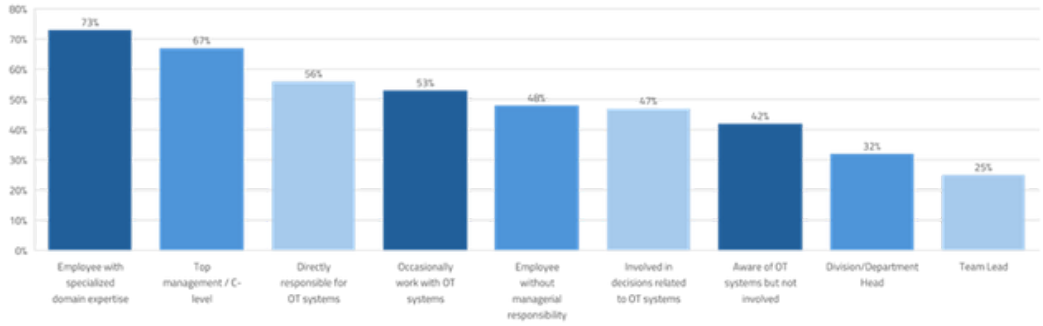
- Advanced Supply Chain Orchestration: Comprehensive planning and resource management systems allow for better prediction and management of disruptions.
- Redundant Operational Systems: Alternative production paths and backup systems enable operational continuity during problems.
- Buffered Production Frameworks: Larger inventories and scheduling flexibility allow for effective absorption of operational disruptions.

COMMUNICATION AND MONITORING FAILURES: THE MID-TIER CHALLENGE

The Maturity Gradient in Monitoring Infrastructure

Communication and monitoring failures were cited by 41% of all respondents, but significant organizational scale-based differences reveal a fascinating pattern of technological maturity:

- High exposure in medium-sized firms: 56% of respondents from companies employing 1,000-5,000 people
- Low vulnerability in large corporations: Only 17% of respondents from enterprises exceeding 5,000 employees



Source: Statista 2025

Transitional Phase vs. Technological Maturity

This suggests a maturity gradient in monitoring infrastructure deployment. Medium-sized organizations are likely in transitional phases, adopting OT visibility solutions whilst still encountering integration or scalability limitations.

Large enterprises appear to have successfully implemented centralized monitoring platforms with substantially reduced exposure to visibility failures.

DATA INTEGRITY: THE HIDDEN THREAT IN UNSTABLE ENVIRONMENTS

Least Recognized but Highly Impactful Risk

Data loss or inaccurate data represented the least frequently selected disruption, cited by 24% of all respondents. However, within organizations characterized as operating somewhat unstable OT environments, this disruption was reported by 39% of respondents.

Data Integrity as Indicator and Amplifier

This finding confirms the concept that data integrity issues serve both as a symptom and amplifier of broader OT system fragility. Data quality problems:

- Signal deeper systemic issues: When data becomes unreliable, it often indicates problems with underlying infrastructure
- Amplify other problems: Inaccurate data makes it difficult to diagnose and resolve other operational issues
- Require prioritization in unstable environments: Organizations with already problematic systems must be particularly vigilant about data quality

DISRUPTION FREQUENCY: STABILITY IN PERCEPTION, VOLATILITY IN EXPOSURE

The Frequency Paradox: Common but Not Chronic

Despite the widespread identification of system downtime and equipment failures as the most frequently cited OT disruption, the perceived frequency of occurrence remains generally low. 36% of all respondents report such disruptions occurring several times a year, annually, or less frequently.

This seemingly paradoxical finding points to an important truth about the nature of OT disruptions: whilst they are common in the sense that most organizations experience them, they are not necessarily persistent operational challenges for the majority of firms.

Risk Segmentation: Rare for Most, Frequent for the Most Exposed

Deeper analysis of frequency perception reveals clear stratification based on OT system exposure and environmental stability.

General population:

- Only 5% of all respondents report downtime occurring several times a month
- 23% of all respondents indicate monthly recurrence

High-risk groups: This monthly recurrence increases significantly within specific subgroups:

- 47% of respondents from companies with somewhat unstable OT environments
- 45% of top management/C-level executives
- 43% of respondents directly responsible for OT systems

Risk Concentration and Executive Awareness

The data highlights risk concentration in unstable OT environments and amongst key technical and strategic stakeholders. Whilst most organizations experience these disruptions sporadically, certain operational contexts face them at frequencies that threaten operational stability.

Particularly significant is C-level awareness of this recurrence pattern, suggesting growing executive recognition of OT fragility, though strategic response mechanisms may still require development.

PRODUCTION DELAYS: EPISODIC BUT WIDESPREAD IMPACT

Predictable Unpredictabilities

The disruption delays in production or operations occurs several times a year for 34% of all respondents, indicating a more episodic impact pattern.

Segmented responses reinforce this trend:

- 67% of companies employing 500-999 people

- 50% of respondents from companies exceeding 5,001 employees

- 40% of companies employing 1,000-5,000 people

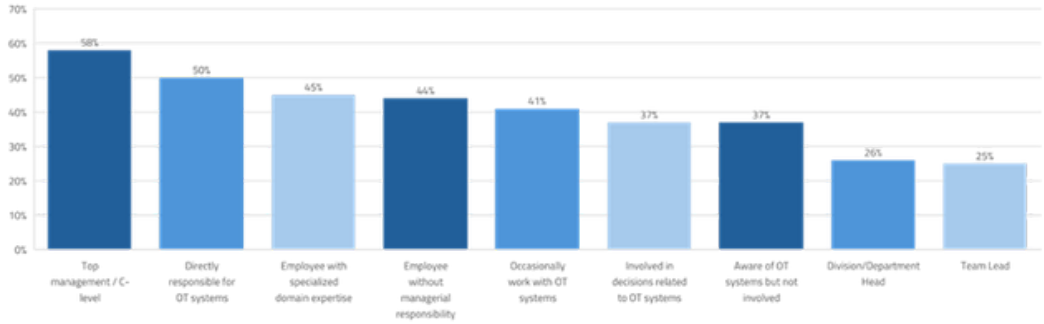
Structural Bottlenecks Across Different Scales

Across diverse organizational scales, production delays are treated as occasional but anticipated events, particularly in mid- and upper-tier size categories. This suggests structural process bottlenecks or inefficiencies that may not demand immediate reengineering attention but cumulatively degrade throughput and operational responsiveness over time.

SAFETY AND COST IMPACT: LOW FREQUENCY, HIGH EXECUTIVE SENSITIVITY

Rare but Potentially Catastrophic Events

The disruption category increased safety risks and operational costs is reported as occurring only several times a year by 70% of all respondents, suggesting infrequent but potentially high-impact events.



Source: Statista 2025

Inverted Perception Pattern

Role-based segmentation reveals notable contrasts that indicate possible reporting and communication problems.

Management perception (infrequent occurrence):

- 100% of top management/C-level executives
- 80% of respondents involved in OT-related decisions

Operational perception (greater variability):

- Only 50% of employees with specialized domain expertise
- 40% ofthose occasionallyinterfacingwithOTsystems

Hidden Costs and Near-Miss Events

A notable inverted perception pattern emerges—strategic leaders view safety and cost-related disruptions as rare occurrences, whilst technical and operational roles observe greater variability. This signals possible underreporting or inadequate communication of near-miss safety events and hidden cost escalations to senior management.

This situation may lead to:

- Distorted risk assessments: Management may not fully understand actual threats
- Delayed implementation of preventive controls: Without full risk awareness, prevention investments may be postponed
- Potentially catastrophic surprises: When actual serious incidents occur, the organization may be unprepared

STRATEGIC IMPLICATIONS: REDEFINING OT RISK MANAGEMENT

For Organizational Leaders

Our findings require a fundamental redefinition of approaches to OT risk management:

- Establishing Transparent Communication Protocols: Organizations must develop mechanisms that ensure information about OT disruptions flows from operational to strategic levels without filtering or trivialization. Investment in Proactive Monitoring:
- Rather than waiting for downtime reports, leaders should implement systems that provide real-time visibility into OT performance.
- Balanced Approach to Budgeting: Preventive costs must be weighed not only against direct disruption costs, but also against hidden costs of lost productivity and competitive erosion.

For Small and Medium Enterprises

The SME segment requires particular attention given their disproportionate exposure:

- Collaborative Risk Management: Smaller firms should consider partnerships or consortia for sharing the costs of advanced OT solutions.
- Critical Asset Prioritization: Rather than trying to modernize everything at once, SMEs should identify and secure their most critical systems.
- Leveraging Cloud-Based Solutions: Cloud-based solutions can provide enterprise-level capabilities without proportional capital investments.

STRATEGIC IMPLICATIONS: REDEFINING OT RISK MANAGEMENT FOR THE ENTIRE SECTOR

Industry must recognizethatOT disruption managementisn't merelya technicalmatter,buta

strategic competitive imperative. Organizations that effectively combine operational resilience with strategic visibility will shape the future of their sectors, whilst those that ignore these warning signals risk marginalization in an increasingly demanding and connected industrial ecosystem.

CHAPTER III:

OT SECURITY SECURING INDUSTRIAL SYSTEMS

The Cybersecurity Reality Check: From Incident Response to Strategic Defence

- Current cybersecurity incident landscape and threat exposure
- Organizational preparedness and confidence levels
- Regulatory compliance awareness and implementation
- Strategic security initiatives and future planning

INTRODUCTION: THE NEW BATTLEGROUND OF INDUSTRIAL CYBERSECURITY

The year 2024 marked a watershed moment foroperational technology security. As industrial systems become increasingly interconnected and digitized, they present an ever-expanding attack surface for cybercriminals and nation- state actors alike. The convergence of IT and OT networks, whilst enabling unprecedented operational efficiency, has simultaneously exposed critical infrastructure to sophisticated cyber threats that were previously confined to traditional enterprise networks.

Our research reveals a sobering reality: whilst organizations express confidence in their cybersecurity preparedness, the frequency and sophistication of actual incidents paint a more complex picture. The gap between perceived readiness and operational reality has become a critical vulnerability that threatens not only individual organizations but entire industrial ecosystems.

This chapter examines three fundamental questions that define the current state of OT cybersecurity: What cyber incidents are actually affecting manufacturing companies? How prepared do organizations believe they are for OT-specific threats? And what concrete measures are being implemented to strengthen industrial defenses?

THE CYBERSECURITY INCIDENT LANDSCAPE: WHAT'S REALLY HAPPENING IN INDUSTRIAL ENVIRONMENTS

Data Breaches and Unauthorized Access: The Predominant Threat

Our research reveals that 71% of respondents experienced data breaches or unauthorized access events within the past year, establishing these incidents as the most prevalent cybersecurity challenge facing industrial organizations. This statistic is particularly alarming when viewed against the backdrop of increasing regulatory scrutiny and the critical nature of industrial data.

The scale of this exposure becomes even more concerning when compared to global cybersecurity trends. Recent reports indicate that manufacturing has become the most targeted industry for cyberattacks, with a 87% increase in incidents year-over-year. The prevalence of data breaches in our survey aligns with this trend, suggesting that OT environments are bearing the brunt of this escalating threat landscape.

The Expertise-Management Perception Gap: A Critical Blind Spot

One of the most striking discoveries in our incident analysis is the dramatic difference in how cybersecurity incidents are perceived across organizational hierarchies:

- Technical specialists' reality: 100% of employees with specialized domain expertise reported experiencing data breaches or unauthorized access events
- Management's perspective: Only 50% of division/department heads acknowledged similar occurrences

This disparity reveals a fundamental communication breakdown that could have catastrophic consequences. When those closest to the technical infrastructure report universal exposure to cyber incidents, whilst middle management acknowledges only half that rate, it suggests either systematic underreporting or dangerous organizational blind spots that could leave organizations vulnerable to unaddressed threats.

Operational Instability as a Cybersecurity Risk Multiplier

The correlation between operational stability and cyber incident frequency reveals a critical security dynamic that has profound implications for industrial risk management:

- Unstable environments: 82% of organizations with somewhat unstable OT environments experienced data breaches
- Stable environments: 60% of organizations with mostly stable operations reported similar incidents

This pattern suggests that operational disruptions create security vulnerabilities through multiple pathways:

- Access control degradation during system interruptions: Emergency procedures often bypass normal security protocols
- Limited visibility in hybrid environments: Legacy systems lacking integrated monitoring become blind spots
- Reactive security postures: Unstable operational contexts often prioritize immediate functionalityover comprehensivethreatmanagement

Malware Infections: The Silent Infiltrator

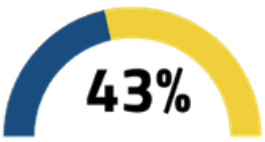
52% of respondents encountered malware infections, positioning this threat as the second most common cybersecurity challenge. This figure is particularly concerning given the potential for malware to spread laterally through interconnected OT networks, potentially disrupting critical operational processes.

The prevalence of malware in industrial environments reflects the increasing sophistication of attackers who understand the unique vulnerabilities of OT systems. Unlike traditional enterprise networks, where malware might primarily target data theft or system disruption, malware in OT environments can directly impact physical processes, creating safety risks and operational havoc.

Insider Threats: The Enemy Within

43% of organizations faced insider threat incidents, highlighting a category of risk that is particularly challenging to address through traditional cybersecurity measures. Insider threats in OT environments are especially dangerous because they often involve individuals with legitimate access to critical systems and deep knowledge of operational processes.

43%
Organizations faced
insider threat incidents



The prevalence of insider threats underscores the importance of comprehensive security frameworks that address not only external threats but also the risks posed by malicious or compromised internal actors.

ORGANIZATIONAL SCALE AND CYBER VULNERABILITY: SIZE MATTERS IN SECURITY

The Mid-Size Enterprise Vulnerability

Unauthorized access incidents demonstrate clear correlations with organizational scale, revealing patterns that challenge conventional assumptions about enterprise security:

- Complete exposure in mid-sized firms: 100% of companies with 500-999 employees reported unauthorized access incidents
- Reduced exposure in larger enterprises: 75% of companies with 1,000-5,000 employees and 67% of companies with 300-499 employees

This pattern suggests that mid-sized organizations may face a perfect storm of cybersecurity challenges: they're large enough to attract sophisticated attackers but may lack the comprehensive security resources available to larger enterprises. They've moved beyond the relative obscurity that might protect very small organizations but haven't yet achieved the security maturity of large corporations.

The Stability-Security Nexus

The relationship between operational stability and cybersecurity exposure reveals a critical insight for risk management:

- Unstable environments - universal exposure: 100% of respondents from somewhat unstable OT environments reported unauthorized access incidents
- Stable environments - reduced vulnerability: Only 40% of mostly stable environments experienced comparable issues

100%
Unstable environments reported unauthorizedaccess

40%
Mostlystable environments faced similar breaches

This correlation reinforces the concept that operational excellence and cybersecurity resilience are inextricably linked. Organizations that achieve operational stability appear to create conditions that naturally resist cyber intrusions, whilst those struggling with operational challenges become more vulnerable to security breaches.

PERCEIVED CYBERSECURITY PREPAREDNESS: CONFIDENCE VS. REALITY

The Confidence Paradox: High Assurance in a High-Risk Environment

Despite the substantial incident exposure revealed in our research, an overwhelming 90% of organizations express confidence in their preparedness to address OT cybersecurity threats. This apparent contradiction between incident frequency and confidence levels reveals a complex dynamic that warrants careful examination.

This high confidence level exists against a backdrop of escalating cyber threats. The 2024 industrial cybersecurity landscape saw a 146% increase in cyberattacks leading to physical operational impairments, with over 1,000 sites affected globally. The disconnect between this threatening environment and organizational confidence suggests either remarkable resilience or concerning overconfidence.

Scale-Based Confidence Patterns: Bigger Means More Confident

Organizational confidence in cybersecurity preparedness demonstrates clear scaling patterns that reflect resource availability and security investment capacity:

- Large enterprise assurance: 100% of companies exceeding 5,001 employees believe they are adequately or highly prepared
- Progressive confidence scaling: 94% of companies with 1,000-5,000 employees and 85% of companies with 300-499 employees

This graduated confidence pattern likely reflects the reality of cybersecurity resource allocation. Larger organizations can afford dedicated cybersecurity teams, advanced monitoring tools, and comprehensive security frameworks that smaller organizations might find financially prohibitive.

Role-Based Preparedness Assessment: The Hierarchy of Realism

Analysis of very prepared responses reveals notable variations across organizational functions that suggest different perspectives on security readiness:

- Technical confidence: 76% of employees with specialized domain expertise and 75% of team leads
- Management caution: 63% of top management/C-level executives and only 57% of division/department heads

76%
Domain experts

75%
Teamleads

63%
Topmanagement / C-level executives

57%
Division/Department heads

The proportionally lower confidence among senior leadership may actually indicate more sophisticated risk assessment perspectives rather than inadequate readiness. C-level executives and department heads are likely more aware of strategic vulnerabilities, regulatory expectations, and thepotential consequences ofsecurity failures.

Operational Stability as a Preparedness Indicator

The relationship between operational stability and security confidence demonstrates stark contrasts that illuminate the connection between operational excellence and cybersecurity readiness:

- Stable environments - high confidence: 99% of respondents from very stable OT environments declare high preparedness
- Declining confidence with instability: 27% from mostly stable environments feel very prepared and just 4% from somewhat stable environments express high confidence

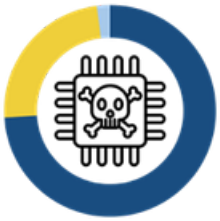
This correlation suggests that operational maturity serves as both a foundation for actual cyber resilience and a driver of organizational confidence in security capabilities. Organizations that have mastered operational stability appear better positioned to address cybersecurity challenges effectively.

REGULATORY AWARENESS AND COMPLIANCE: KNOWLEDGE CONCENTRATION AND GAPS

High Self-Assessed Regulatory Knowledge

A substantial 74% of respondents consider themselves highly knowledgeable regarding major cybersecurity frameworks and regulations such as NIS2, NIST, or ISO 27001. Additionally, 24% consider themselves very familiar with applicable frameworks, leaving only 2% rating themselves as somewhat familiar.

24%
Respondents whoarevery familiar with applicable regulations



74%
Respondents consider themselves highly knowledgeable about cybersecurity frameworks

This high level of self-assessed regulatory knowledge suggests that cybersecurity frameworks have achieved significant penetration in industrial organizations. However, the distribution of this knowledge across organizational functions reveals potential vulnerabilities in compliance implementation.

Executive-Technical Knowledge Concentration

Regulatory knowledge concentration varies significantly across organizational functions, revealing a pattern that could impact compliance effectiveness.

High-level expertise:

- 96% of top management/C-level executives report high knowledge levels
- 78% of employees with specialized domain expertise demonstrate similar confidence

Mid-level knowledge gaps:

- 67% of division/department heads
- Only 56% of team leads

96%
Topmanagement / C-level executives

78%
Domain experts

67%
Division/Department heads

56%
Teamleads

This concentration of regulatory knowledge at the executive and technical specialist levels, whilst leaving mid-level management with lower familiarity, could create implementation gaps. Division heads and team leads are often responsible for translating high-level compliance requirements into operational procedures, making their knowledge level critical for effective compliance.

Operational Context and Regulatory Understanding

Environmental stability appears to influence self-assessed regulatory understanding, revealing another dimension of the stability-security relationship.

Stable environment advantages: In very stable OT environments:

- 88% report high regulatory knowledge
- 12% are very familiar

Instability-knowledge correlation: In somewhat unstable OT environments:

- Only 61% feel highly knowledgeable
- 30% are very familiar
- 9% acknowledge being somewhat familiar

This correlation suggests that organizations facing operational disruptions may struggle to build comprehensive compliance competencies, potentially creating regulatory vulnerabilities alongside their operational challenges.

REGULATORY IMPACT: CYBERSECURITY MANDATES AS TRANSFORMATION CATALYSTS

Driving Fundamental Security Improvements

Cybersecurity regulations are exercising substantial influence on organizational OT security approaches, with 82% of all respondents reporting that regulations have directly influenced:

- Security audit procedures
- Incident response preparedness
- Employee cybersecurity training programmes

This high level of regulatory influence demonstrates that compliance frameworks are successfully driving practical security improvements across industrial organizations. The fact that over four-fifths of organizations report direct regulatory influence suggests that mandates are translating into operational changes rather than remaining as paper exercises.

Role-Specific Regulatory Influence Patterns

The intensity of regulatory influence varies significantly by organizational role, revealing interesting patterns in how compliance requirements permeate organizations

- Operational level engagement: 94% of team leads and 85% of non-managerial employees
- Executive level detachment: Only 67% of top management/C-level executives

This inverted pattern, where operational personnel report higher regulatory influence than executives, suggests that compliance requirements are being felt most acutely by those responsible forimplementationrather than thosesetting strategic direction.

Strategic IT-OT Integration Acceleration

78% of respondents indicate that regulations are driving closer integration of IT and OT security strategies, representing a fundamental shift in how organizations approach industrial cybersecurity. This integration is critical given the increasing convergence of operational and information technology systems.

Organizational scale breakdown reveals interesting patterns:

- 91% of companies with 500-999 employees

- 90% of companies exceeding 5,001 employees

- Only 74% of companies with 300-499 and 1,000-5,000 employees

The higher integration rates among mid-sized and very large companies, with lower rates among small and large enterprises, suggests that regulatory pressure affects different organizational sizes incomplex ways.

Investment and Security Control Enhancement

Regulations are driving concrete investments across critical security domains:

- 75% report increased investment in: OT cybersecurity solutions, Compliance framework implementation, Governance capability development
- 74% are strengthening OT-specific controls, including: Threat detection system deployment, Access control protocol enhancement, Network segmentation implementation

These investment patterns demonstrate that regulatory frameworks are successfully translating into tangible security improvements rather than merely compliance theatre.

CURRENT SECURITY STRATEGY IMPLEMENTATION: PROACTIVE MEASURES AND EXECUTION GAPS

Supply Chain Security: The Top Strategic Priority

74% of all respondents report organizational steps to strengthen supply chain and external security, establishing this as the most commonly implemented strategic initiative. This prioritization reflects growing awareness that OT security extends far beyond organizational boundaries to encompass entire industrial ecosystems.

The focus on supply chain security is particularly relevant given recent high-profile attacks that leveraged supplier relationships to infiltrate target organizations.

Role-based implementation patterns:

- 88% of team leads
- 78% of specialized domain experts
- Only 67% of division/department heads

88%
Teamleads

78%
Domain experts

67%
Division/Department heads

The lower implementation rate among division heads, who often serve as the bridge between strategic direction and operational execution, could represent a critical gap in organizational security coordination.

Operational Resilience and Continuity Planning

67% of all respondents report implementation of resilience and backup planning strategies, establishing this as the second most adopted measure. This focus on operational continuity reflects the unique nature of OT environments, where system availability can be as critical as system security.

Scale-based implementation reveals resource disparities:

- 83% of companies with 5,001+ employees
- 77% of companies with 500-5,000 employees
- Only 57% of companies with 300-499 employees

Role-based patterns show concerning executive disengagement:

- 78% of specialized domain experts
- 73% of non-managerial employees
- Only 48% of top management/C-level executives

The combination of lower implementation rates among smaller organizations and reduced executive engagement could create significant vulnerabilities in industrial resilience.

Comprehensive Security Framework Implementation

Additional strategic implementation areas demonstrate broad-based security improvements:

- Network and access security — 65%
- Cybersecurity training & IT/OT collaboration — 64%
- Continuous risk assessment & system monitoring — 63%

These figures suggest that organizations are pursuing comprehensive approaches to OT security rather than focusing on isolated solutions.

FUTURE OT SECURITY STRATEGY: THREE-YEAR ROADMAP AND STRATEGIC ALIGNMENT CHALLENGES

Technology Modernization as the Primary Future Focus

38% of all respondents plan new OT technology adoption within the next three years, representing the top strategic priority for future development. However, this strategic intent reveals significant organizational alignment challenges:

- Team lead enthusiasm: 69% of team leads are driving technology adoption plans
- Executive hesitation: 41% of non-managerial employees and only 30% of top management/C-level executives

This dramatic difference in strategic vision between operational leaders and senior executives could create implementation challenges and resource allocation conflicts.

Legacy Infrastructure Modernization: The Overdue Priority

32% plan to prioritize legacy infrastructure modernization and system maintenance, representing a critical but underinvested area. The relatively low prioritization of this fundamental requirement may reflect budget constraints or competing priorities.

Adoption patterns by OT familiarity reveal interesting dynamics:

- 40% of those aware of OT systems but not directly involved
- 37% who occasionally interface with OT systems
- Only 18% of those involved in OT decision-making processes

40%
Aware of OTsystems
but not involved

37%
Occasionallywork
with OT systems

18%
Involved indecisions
related to OT systems

The lower prioritization among decision-makers could indicate either confidence in existing infrastructure or insufficient awareness of legacy system vulnerabilities.

Network and Access Security Strengthening

Planned by 26% of respondents overall, this critical security domain shows clear scale-based patterns:

- 31% of companies with 5,001+ employees

- 29% of companies with 1,000-5,000 employees

- Only 18% of companies with 500-999 employees

The lower prioritization among mid-sized companies is concerning, given their higher reported exposure tounauthorizedaccessincidents.

Continuous Risk Assessment and System Monitoring

Also planned by 26% of all respondents, this strategic area shows interesting engagement patterns.

Higher interest among:

- 37% of specialized domain experts
- 32% of companies with 300-999 employees
- 43% from companies with somewhat unstable OT environments

Lower engagement from:

- Only 9% from companies with 1,000-5,000 employees
- 19% of team leads

The high interest from unstable environments suggests that organizations experiencing operational challenges recognize the need for enhanced monitoring, whilst more stable organizations may feel less urgency.

STRATEGIC IMPLICATIONS: BRIDGING THE SECURITY-OPERATIONS DIVIDE

For Senior Leadership

Our findings reveal critical leadership challenges that require immediate attention:

- Address the Perception-Reality Gap: The disconnect between high confidence levels and actual incident exposure suggests that leadership may not have complete visibility into their organization's cyber risk profile. Bridge Executive-Operational Strategy Alignment:
- The significant differences in future planning enthusiasm between executives and operational teams could undermine implementation effectiveness. Invest in Middle Management Capability: The knowledge
- and implementation gaps at the division head level represent a critical vulnerability in organizational security coordination.

For Mid-Sized Organizations

The research reveals that companies with 500-999 employees face particular challenges:

- Universal Unauthorized Access Exposure: With 100% reporting such incidents, this segment requires immediate and comprehensive security intervention.
- Resource Optimization: These organizations must find ways to achieve enterprise-level security capabilities without proportional resource investments.
- Regulatory Compliance Support: Lower regulatory knowledge levels suggest this segment may benefit from external compliance support or industry collaboration initiatives.

For the Industrial Ecosystem

The research points to systemic challenges that require industry-wide responses:

- Supply Chain Security Coordination: With 74% prioritizing supply chain security, industry-wide standards and coordination mechanisms become critical.
- Information Sharing Enhancement: The communication gaps between technical specialists and management suggest that industry-wide threat intelligence sharing could improve organizational awareness.
- Regulatory Framework Effectiveness: Whilst regulations are driving improvements, the uneven implementation across organizational levels suggests that regulatory approaches may need refinement.

LOOKING FORWARD: THE CONVERGENCE IMPERATIVE

Theevidence suggeststhat thefuture of OTsecurityliesin successfully convergingoperational excellence with cybersecurity resilience. Organizations that achieve this convergence—evidenced by the correlation between operational stability and security preparedness—will be best positioned to thrive in an increasingly connected and threatened industrial landscape.

The path forward requires not just technological investment, but fundamental changes in organizational communication, strategic alignment, and risk management approaches.
The stakes could not be higher: in an era where cyber incidents can cause physical operational disruptions affecting millions of people, the difference between cyber-resilient and cyber-vulnerable organizations may well determine which industrial enterprises survive and prosper in the decades to come.

CHAPTER IV:

OT DEVELOPMENT TECHNOLOGY INVESTMENT AND INNOVATION IN OT

Strategic Transformation Directions: Technologies Defining the Future of Industry

- Three-year technology investment priorities and planning
- Emerging trends shaping industrial transformation
- Strategic actions for enhancing automation and competitiveness
- Recommendations for different organizational scales and contexts

INTRODUCTION: INDUSTRY AT THE THRESHOLD OF TECHNOLOGICAL REVOLUTION

Contemporary industry findsitself atatechnologicalinflection point, where investment decisions made today will determine organizational competitiveness for the next decade. As industrial organizations grapple with the mounting operational and cybersecurity challenges analyzed in previous chapters, they must simultaneously plan strategically for the adoption of technologies that will define their future.

Our research reveals a fascinating landscape of industrial transformation:

organizations demonstrate widespread enthusiasm for technological innovation, yet implementation of these visions encounters significant barriers related to organizational alignment, enterprise scale disparities, and differences in priority perception across management levels.

This chapter addresses three fundamental questions shaping the future of

industrial competitiveness: Which technologies—artificial intelligence, edge computing, digital twins—are investment priorities for the next three years? Which trends and innovations will have the greatest impact on OT production and security? And what strategic actions will enable organizations not only to keep pace with change, but also to enhance automation and achieve competitive advantage?

OT TECHNOLOGY IMPLEMENTATION PIPELINE: THREE-YEAR STRATEGIC PLANS

Predictive AnalyticsandPredictiveMaintenance:Universal Strategic Priority

88% of all respondents plan to implement predictive maintenance technologies and real-time analytics platforms, establishing them as the most widely anticipated category of OT development. This overwhelming majority signals a fundamental evolution in industrial asset management—from reactive maintenance models to proactive, data-driven performance management strategies.

The significance of this trend extends beyond technical aspects. McKinsey Global Institute indicates that organizations implementing predictive maintenance achieve a 10-40% reduction in maintenance costs, 20% increase in uptime, and 50% reduction in unexpected equipment failures. These economic realities explain why predictive analytics is evolving from a technological option into a baseline operational expectation.

Organizational Support Patterns: Enthusiasm vs. Pragmatism

Particularly strong support amongst:

- 94% of team leads
- 92% of those aware of OT systems but not directly involved in operations
- 93% of companies operating very stable OT environments

Support diminishes amongst:

- 81% of division/department heads
- 79% of companies with mostly stable operational environments

This disproportion reveals an interesting pattern: the highest enthusiasm is shown by those closest to operational reality (team leads) and those with strategic perspective without direct operational responsibility. Division heads, often responsible for implementation budgets and project risk management, demonstrate greater caution—likely due to awareness of the complexity and costsassociatedwith technological transformation.

Stability as the Foundation for Innovation

Particularly significant is the discovery that organizations with very stable OT environments (93%) show the highest support for predictive technologies. This confirms a key thesis from our earlier analyses: operational stability does not lead to complacency, but creates a solid foundation for further innovation. Organizations that have mastered operational excellence are better prepared for successful adoption of advanced technologies.

FULLY AUTONOMOUS PRODUCTION LINES: AMBITIOUS VISION WITH IMPLEMENTATION CHALLENGES

Executive-Driven Initiative with Dramatic Organizational Chasm

81% overall express intent to implement autonomous production line capabilities, representing one of the most ambitious categories of industrial transformation. This technology does not constitute evolutionary change—it is a revolutionary transformation of the nature of industrial production, where human intervention becomes the exception rather than the rule.

81%
Organizations planning to implement autonomous production lines

Highest support from: 96% of top management/C-level executives

Significantly diminished enthusiasm amongst middle management: Only 60% of division/ department heads.

Anatomy of a 36-Point Strategic Chasm

This dramatic difference in enthusiasm between executive leadership and middle management represents one of the widest gaps in our entire study. This disconnect reveals a fundamental challenge in strategic communication and organizational alignment.

C-level leadership, likely influenced by competitive pressure and long-term strategic vision, perceives autonomy as a critical element of future competitiveness. Middle management, responsible for practical implementation, may be more aware of operational challenges, transformation costs, and risksassociated with such radical changes to production processes.

Economic Imperatives Driving Executive Enthusiasm

Executive enthusiasm for autonomous production lines finds economic justification. Boston Consulting Group indicates that fully autonomous production systems can increase productivity by 30-50%, reduce quality defects by 40-90%, cut operational costs by 25-45%, and improve safety metrics by 70-90%. These transformative potentials explain why autonomy has become a strategic imperative for executive leadership, despite implementation complexities and middle management hesitation.

OT-TAILORED CYBERSECURITY ENHANCEMENTS: CRITICAL SCALE-DEPENDENT IMPLEMENTATION GAPS

High Intent, Concerning Implementation Disparities

81% of respondents plan to implement OT-specific cybersecurity improvements, including threat detection systems, network segmentation, and access control protocols.

81%
Organizations planning OT-specific cybersecurity improvements

Adoption Patterns by Organizational Scale: Unexpected Vulnerabilities

Adoption by organizational scale reveals a concerning pattern:

- 89% of companies employing 1,000-5,000 people
- Only 68% of companies employing 500-999 people

This finding is particularly alarming in the context of earlier discoveries, which showed that companies employing 500-999 people experienced a 100% rate of unauthorized access incidents. The segment with the highest cybersecurity exposure demonstrates the lowest investment intent for OT-specific cybersecurity solutions—creating potential systemic vulnerability for entire industrial supply chains.

The Risk-Investment Paradox: Understanding the Disconnect

This paradox may reflect several critical factors:

- Resource Constraints vs. Risk Reality: Mid-sized companies may recognize cybersecurity necessity but lack financial resources for comprehensive OT security implementations.
- Complexity Overwhelm: The complexity of implementing OT cybersecurity solutions can be paralyzing for organizations with limited technical resources and expertise.
- Risk Normalization Syndrome: Organizations that have repeatedly experienced incidents may develop harmful risk normalization, treating cyber incidents as „cost of doing business" rather than addressable threats.

This situation requires urgent ecosystem-wide attention, as cybersecurity in OT environments has an inherently systemic character—the weakness of one organization can compromise entire industrial networks and supply chains.

EMERGING OT TRENDS: CYBERSECURITY, CONVERGENCE, AND AI AS INNOVATION CATALYSTS

Enhanced OT Cybersecurity Measures: Most Anticipated Transformation

83% of all respondents identify OT cybersecurity advancement as the most impactful trend trajectory over the next three years. This discovery confirms that cybersecurity has evolved from a technical concern to a strategic imperative for the entire industrial sector.

Particularly emphasized by:

- 91% of respondents from companies employing 500-999 people
- 94% of team leads
- 93% of those with specialized domain expertise

Support weakens amongst:

- Only 72% of companies exceeding 5,001 employees
- Just 67% of division/department heads

Large Enterprise Cybersecurity Confidence: Strategic Overconfidence or Resource Buffering?

Lower cybersecurity prioritization amongst the largest enterprises may reflect several phenomena: strategic overconfidence from existing cybersecurity investments, greater operational resource buffering capabilities that reduce perceived urgency for cybersecurity enhancements, or implementation complexity in very large organizations leading to more cautious approaches.

Strengthened IT-OT Convergence and Collaborative Integration

81% overall anticipate that increased IT-OT integration will deliver significant operational impact, representing a fundamental shift in the organizational architecture of contemporary industry.

Particularly recognized by:

- 93% with specialized domain expertise
- 89% of those aware of OT systems but not directly involved in operations

Again, only 67% of division/department heads foresee this level of impact, highlighting persistent mid-tier management engagement gaps that may undermine convergence initiatives.

AI and Machine Learning Integration in OT Systems

Selected by 77% of respondents, reflecting growing organizational confidence in AI's operational value proposition. This represents a tipping point where artificial intelligence transitions from experimental technology to mainstream operational tool:

Highest enthusiasm from:

- 91% of companies employing 500-999 people
- 89% of top management/C-level executives
- 91% of companies with somewhat unstable OT environments

Support demonstrates weakness from:

- 67% of division/department heads
- 73% of companiesemploying300-499people

Unstable Environments as AI Adoption Catalyst

Particularly intriguing is the discovery that organizations with somewhat unstable OT environments (91%) show the highest enthusiasm for AI integration. This suggests that operational challenges may serve as a catalyst for innovative technology adoption, with organizations viewing AI as a potential solution to their stability issues.

STRATEGIC VISION FRAGMENTATION: COMMUNICATION AND ALIGNMENT CHALLENGES

Consistent Pattern of Division/Department Head Disconnection

The most striking pattern in our data is the consistent disconnection of division/department heads from strategic technology trends. In every major category—cybersecurity (67%), IT-OT convergence (67%), AI/ML (67%)—this management level demonstrates significantly lower engagement than both executive leadership and technical teams.

Organizational Implications of the Middle Management Gap

This persistent gap may have serious consequences for technology strategy implementation:

- Strategic Filtering Effect: Division heads often serve as the crucial bridge between strategic vision and operational implementation. Their lower engagement may lead to dilution or distortion of strategic initiatives. Resource Allocation Bottlenecks: Without full
- middle management support, technology transformation projects may struggle with inadequate resource allocation or prioritization. Change Management Resistance: Effective technology transformation
- requires support at all organizational levels. Lack of middle management engagement may undermine change management initiatives and employee adoption. Communication Breakdown: The
- middle management gap may indicate broader communication issues between senior leadership's strategic planning and operational implementation responsibilities.

STRATEGIC ACTIONS FOR ENHANCING AUTOMATION AND COMPETITIVENESS

For Organizational Leaders: Critical Strategic Imperatives

Our findings indicate several key strategic actions that organizations must undertake to effectively navigate technological transformation:

1. Bridging the Middle Management Engagement Gap

Organizations must actively address the middle management engagement gap through:

- Executive Communication Strategy: Regular, structured communication with middle management about technology strategy rationale and expected benefits
- Technology Leadership Development: Dedicated programmes developing middle managers as technology champions within their departments
- Cross-Functional Integration Teams: Mixed teams combining executive leadership, middle managers, and technical specialists for collaborative technology planning

2. Phased Implementation Strategy for Technology Adoption

Rather than attempting simultaneous implementation of all technologies, organizations should adopt a structured, phased approach:

Phase 1 - Foundation Building (Year 1):

- Stabilization of core OT systems and infrastructure
- Implementation of basic predictive analytics capabilities
- Establishment of baseline cybersecurity measures

Phase 2 - Advanced Capabilities (Year 2):

- Deployment of advanced cybersecurity systems and threat detection
- Implementation of edge computing and real-time analytics platforms
- Commencement of AI/ML pilot programmes in controlled environments

Phase 3 - Autonomous Systems Preparation (Year 3):

- Advanced AI/ML integration in production systems
- Preparation for autonomous production line capabilities
- Full implementation of IT-OT convergence

3. Collaborative Ecosystem Development Strategies

Particularly for mid-sized enterprises that may lack resources for independent transformation, developing collaborative approaches is crucial:

- Technology Partnerships: Strategic alliances with solution providers offering scalable, cost-effective implementations
- Industry Consortiums: Collaborative arrangements for sharing R&D costs and best practices
- Academic Collaboration: Partnerships with research institutions for access to cutting-edge technology development

For Mid-Sized Enterprises: Critical Priority Actions

The segment employing 500-999 people requires particular strategic attention given their unique vulnerabilities:

Cybersecurity Prioritization as Strategic Imperative

Despite resource constraints, OT cybersecurity investments cannot be deferred given the 100% incident rate in this segment:

- Cloud-Based Security Solutions: Leveraging cloud solutions offering enterprise-level security without proportional capital investments
- Managed Security Services: Considering outsourcing of specific cybersecurity functions to specialized providers
- Industrial Threat Intelligence Participation: Active participation in industry-wide threat information sharing programmes

AI as Competitive Advantage Lever

High AI engagement in this segment can be leveraged as competitive advantage:

- Focused Use Case Selection: Concentration on specific AI applications where immediate ROI can be demonstrated
- Startup Partnerships: Strategic alliances with AI startups for access to cutting-edge technology without major internal investments
- Targeted Capability Development: Development of internal AI capabilities through focused hiringandtargetedtraining programmes

For Large Enterprises: Ecosystem Responsibility and Leadership

The largest organizations, with substantial resources and capabilities, bear broader ecosystem responsibilities:

- Technology Leadership and Industry Development: Large firms should pioneer the development and deployment of new technologies, creating case studies and best practices for smaller organizations.
- Supply Chain Cybersecurity Orchestration: As hubs for complex supply chains, large organizations must ensure that suppliers and partners also maintain appropriate cybersecurity standards, potentially providing support and resources for smaller suppliers.
- Industrial Talent Development: Investment in technology talent development, not only for their own needs but for building a qualified professional pool for the entire industry.

FUTURE TECHNOLOGY IMPERATIVES: EDGE COMPUTING, DIGITAL TWINS, AND IOT

Edge Computing as Real-Time Processing Foundation

Whilst not explicitly featured in our primary data, edge computing represents a critical supporting technology for all planned investments. The ability to process data close to its source of generation becomes fundamental for effective implementation of predictive analytics and autonomous systems.

Digital Twins as Simulation and Optimization Platforms

Digital twin technology, though not directly mentioned in the study, constitutes a key infrastructure element supporting both predictive analytics and preparation for autonomous production lines. These virtual representations of physical assets enable testing and optimization without risk to actual operations.

Industrial IoT as Sensor Network

The expanding network of IoT devices in industrial environments creates the foundation for all planned technological improvements, from predictive analytics to cybersecurity systems. Organizations must treat IoT not as a separate technology, but as an integral part of their digital transformation strategy.

CONCLUSIONS: CONVERGENCE AS THE KEY TO FUTURE SUCCESS

Ourcomprehensive research reveals thatfutureindustrialsuccesswillbelongto organizations that effectively achieve convergence between operational excellence and technological innovation. These organizations will be characterized by:

- Integrated Strategic Execution: Effective translation of executive vision into operational reality through engaged and competent middle management, eliminating the 36-point gap between C-level enthusiasm and operational implementation.
- Technology as Excellence Accelerator: Utilising advanced technologies - from predictive analytics to AI—to enhance rather than replace fundamental operational disciplines and quality management practices.
- Responsible Ecosystem Leadership: Active participation in industry-wide transformation, with particular emphasis on supporting mid-sized organizations facing the greatest challenges in technological investment and cybersecurity.
- Adaptive Resilience in an Uncertain Environment: The ability to rapidly adapt to changing technological and market conditions whilst maintaining operational stability—a crucial skill in an era of accelerated digital transformation.

Organizations that master this convergence will not only survive but will define the future of industry in an increasingly competitive and technology-driven economic landscape. Those that fail to develop these capabilities risk marginalization in an economy where technological competencies increasingly determine competitive advantage.

The path forward demands unprecedented levels of strategic thinking, implementation discipline, and commitment to building organizational consensus. But for organizations ready to undertake this transformational journey, the rewards—in terms of operational efficiency, competitive position, disruption resilience, and sustainable growth—will define the industrial leaders of the next decade.

EFA AUTOMAZIONE

Proud member of RELATECH

AMDT is the global leader in backup, version control, and comparison solutions for industrial automation, built on nearly 40 years of specialized expertise.

Our mission, "Production Resilience Delivered," reflects our commitment to ensuring that automated production systems are secure, resilient, and capable of fast recovery from disruptions, thereby safeguarding production output. Established in 2022 through the merger of AUVESY GmbH and MDT Software Inc., AMDT is headquartered in Landau, Germany, with offices in the USA and China. Our extensive global network includes over 100 partners, and we proudly support more than 3,000 customers worldwide, helping them maintain optimal performance and resilience in their production environments.

www.octoplant.com