octoplant

EFA AUTOMAZIONE | Proud member of RELATECH

REPORT

+ TRANSFORMATION AND CHALLENGES IN OT SECURITY

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

TABLE OF CONTENT

FOREWORD

The global industrialsectoris undergoing one of the most profound transformations in its history. As digitalization accelerates, operational technology (OT) environments—once separated from enterprise IT systems—have become fully entwined with digital networks and data-driven processes. This convergence fuels innovation, operational efficiency, and intelligent automation, but it also exposes critical systems to unprecedented security risks and systemic vulnerabilities.

Over the past year, the industrial world has faced a complex duality: rapid technological advancement alongside escalating cyber and operational threats. Nearly three-quarters of industrial organizations have reported significant OT-related incidents, and the frequency of system disruptions tied to human error and interoperability challenges continues to rise. Meanwhile, advances in AI-driven analytics, edge computing, and automation are redefining how industries monitor, secure, and optimize their production ecosystems.

This report explores the evolving state of global operational technology security, combining quantitative data with qualitative insights from across sectors and markets. It identifies where maturity and preparedness are strongest, where gaps persist, and how organizations can effectively navigate the changing regulatory and technological environment shaping tomorrow's industrial operations.

The insights presented within these chapters aim to equip leaders with a strategic understanding of transformation pathways that reconcile innovation with resilience. Those who act decisively—integrating cybersecurity, compliance, and agility into the core of their OT systems—will not only safeguard continuity but also seize the competitive edge in an increasingly intelligent industrial age.

In an era marked by rapid digital transformation and increasing reliance on operational technologies (OT), industries worldwide face unprecedented sets of challenges and opportunities. Innovations in industrial technologies, growing cyber risks, and evolving regulatory landscapes compel organizations to continuously evolve their OT security management practices.

This report synthesizes the latest data and insights to present a detailed panorama of the current OT ecosystem, projected technological advancements, and key security challenges shaping the industry's future. It is designed to support decision-makers in making informed, strategic choices that enhance OT security resilience and operational excellence.

The study was conducted by Statista with a sample of 535 respondents representing industrial organizations of various sizes. Participants came from companies employing between 300 and more than 5,000 people, with 19% working in organizations with 300–499 employees, 16% in companies with 500–999 employees, 34% in enterprises with 1,000–5,000 employees, and 32% in large organizations with more than 5,000 employees.

The respondent group reflected a broad cross-section of professional roles and responsibilities within the industrial sector. Eleven percent of respondents held top management or C-level positions, 32% were heads of divisions or departments, 10% served as team leads, 22% were employees without managerial responsibilities, and 25% were domain experts with specialized knowledge.

In terms of functional specialization, 44% identified as cybersecurity analysts or consultants, 11% as engineers or technicians, 17% as IT managers, and another 17% as OT managers. Among senior management, 76% held the title of Chief Technology Officer (CTO), 21% were Chief Information Security Officers (CISO), and 2% each were Chief Data Officers (CDO) and Chief Operating Officers (COO).

Respondents represented various industrial sectors, with the largest shares coming from manufacturing and industrial firms (29%), the chemicals, pharmaceuticals, and life sciences sector (25%), and the energy, utilities, and natural resources sector (18%).

This diverse participant base provides a comprehensive view of the challenges and state of cybersecurity and operational management across different types of industrial organizations.

EXECUTIVE SUMMARY

Despite advances in technology and security awareness, OT environments remain vulnerable to a spectrum of cyber incidents, with data breaches topping the list globally (70%)—most notably in the US (78%) and other regions (71%), while Germany experiences higher malware infection rates (75%). Incident types vary regionally, reflecting different levels of infrastructure maturity and security strategies.

Readiness levels are generally high, particularly among large enterprises and those with stable OT infrastructures, though confidence varies according to organizational roles and operational contexts, underscoring the need for deeper engagement within operational teams.

Compliance with cybersecurity regulations such as ISO 27001, GDPR, and NIS2 is a major driver of enhancement actions across organizations. Adoption rates and regulatory emphasis differ by geography and company size, emphasizing the importance of market-tailored compliance strategies.

Looking ahead, companies are prioritizing investments in emerging technologies such as AI, blockchain, 5G, edge computing, and digital twins to address growing security and efficiency demands. Planned initiatives focus on cybersecurity reinforcement, infrastructure modernization, and automation to ensure competitive advantage in an increasingly digital industrial age.

Ultimately, this report offers vital intelligence and guidance to support the development of future-proof OT environments that balance cutting-edge innovation with operational security and regulatory adherence.

CHAPTER I

THE OT ENVIRONMENT L AN DSCAPE

Where digital maturity defines industrial competitiveness

- Comparative analysisofOT maturitylevels by geography, company size, and organizational role
- Centralized asset inventory automation and its correlation with operational stability
- Foundational and specialized OT technology adoption patterns across industrial roles
- Role-based differences in device management, maintenance frequency, and stability perception

CHARTING THE MATURITY JOURNEY OF INDUSTRIAL TECHNOLOGY

In an era defined by automation and interconnectivity, operational technology forms the backbone of industrial performance. Understanding how organizations evolve from manual oversight to fully automated ecosystems reveals much about their readiness for future innovation. This chapter captures the reality of industrial transformation—where legacy systems meet digital ambitions - and investigates how enterprises translate modernization into measurable resilience.

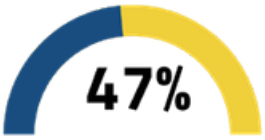
The following analysis offers a nuanced comparison of key operational technology (OT) trends across regions, company sizes, and organizational roles, drawn from the latest comprehensive data sets. It highlights not only the raw adoption figures but also explores what these patterns imply for maturity, operational resilience, and future investment in OT security.

CENTRALIZED OT ASSET INVENTORY: AUTOMATION LEVELS BY GEOGRAPHY, COMPANY SIZE, AND STABILITY

Almost half (47%) of surveyed organizations have achieved full automation of their centralized OT asset inventories, yet more than half still rely on hybrid models blending automated and manual processes. Notably, Germany leads in full automation (57%), closely followed by the US (54%), while other European countries trail considerably at 33%.

47%

Organizations with fully automated, centralized OT asset inventories



Company size is a decisive factor: the largest enterprises (5,001+ employees) demonstrate widespread automation adoption (87%), a testament to the scalability and operational efficiency benefits they capture. However, smaller firms (500–999 employees) lag behind, with a mere 12% fully automated, signaling an area ripe for improvement. Here, regional disparities persist, with "other" countries exhibiting higher adoption (32%) than Germany (5%) or the US (4%). The findings suggest a pronounced maturity gap driven by resource availability and organizational complexity.

- **Large enterprises:**

- **Mid-market:**

- **Small organizations:**

A closer look at roles reveals operational-level employees in Germany embrace automation extensively (76%), indicative of grassroots digital integration. In contrast, US domain experts lead adoption (76%), whereas some European peers remain more tentative (46%). Even among respondents only aware of OT systems but not directly involved, automation is surprisingly prevalent, especially in Germany (75%) and the US (65%). The strong correlation between operational stability and automation levels—peaking at near 80% in very stable environments—underscores the critical role of process dependability in motivating digital investments.

Hybrid approaches remain predominant outside the largest cohorts, especially among smaller firms that face budget or structural constraints. Leadership preferences vary by geography: European top management tends toward hybrids, while American team leads adopt them most frequently. This nuanced landscape reveals hybrid models as pragmatic bridging solutions where full automations prove challenging.

This data paints a clear maturity divide shaped by geography and company size. Large organizations, particularly in Germany and the US, capitalize on the transformative power of automation, gaining precision and responsiveness unavailable to smaller counterparts who remain tethered to manual methods. Operational stability appears to be both a cause and consequence of automation investments. For OT Security leaders, these trends highlight priority segments for digital acceleration and the need for flexible integration models accommodating diverse organizational realities.

OT HARDWARE AND SOFTWARE ADOPTION: UNIVERSAL SYSTEMS AND EMERGING GAPS

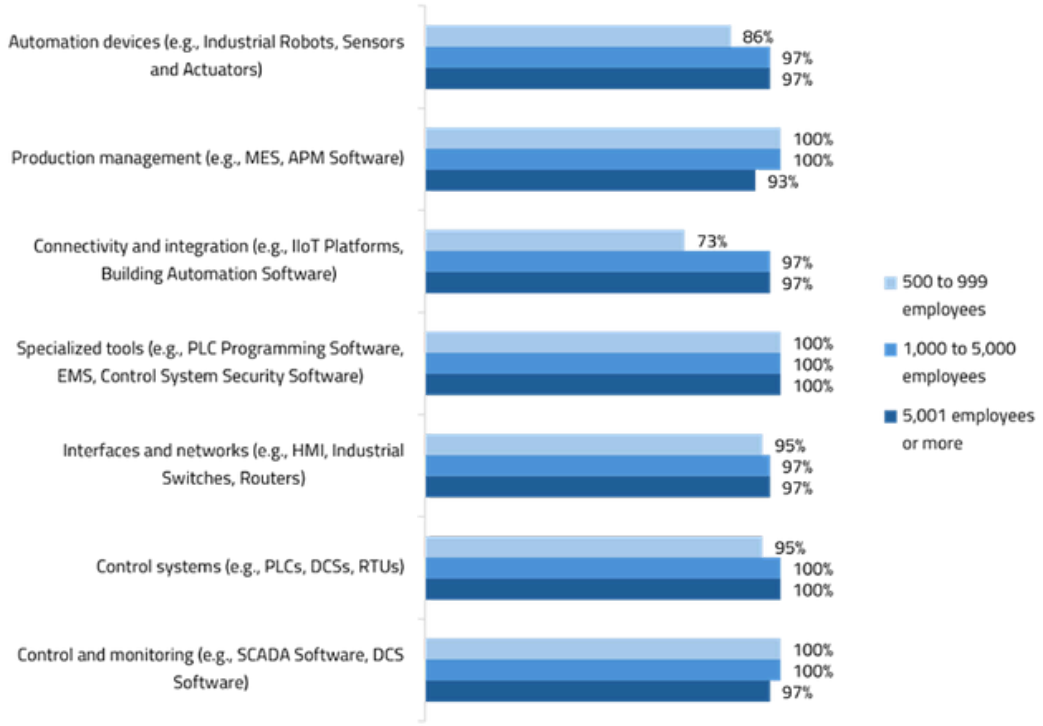
Foundational OTtechnologies,such asHMIs, industrial switches, and routers, enjoy nearly universal adoption (98%), reaching saturation among core operational roles. Control systems (PLCs, DCSs, RTUs) and associated monitoring software are close behind (97%), underscoring their indispensable role in production and process oversight worldwide.

Cross-regional comparisons reveal strong consensus in core technology use, with Germany exhibiting full role-based saturation and the US maintaining robust but more variable deployment, particularly among moderate OT users. The subtle dip in adoption within unstable US environments (down to 50%) signals that operational turbulence can limit technology penetration.

Automation devices, spanning robots and sensors, expose a pronounced regional gap: Germany (93%) and “other” countries (90%) lead while the US (82%) shows weaker uptake. German operational teams achieve blanket adoption, contrasting with a 67% adoption rate among US team leads, pointing to skill or capital barriers.

98%
Use foundational OT interfaces and networkdevices

97%
Usecontrolsystems and monitoring software



Specialized OT tools—PLCs programming, EMS platforms, security utilities—are near-ubiquitous in Germany (99%), with slightly lower yet substantial presence elsewhere. Similarly, infrastructure systems (smart grids, building management) are widely deployed but display modestly lower adoption in other countries, indicating areas for maturation.

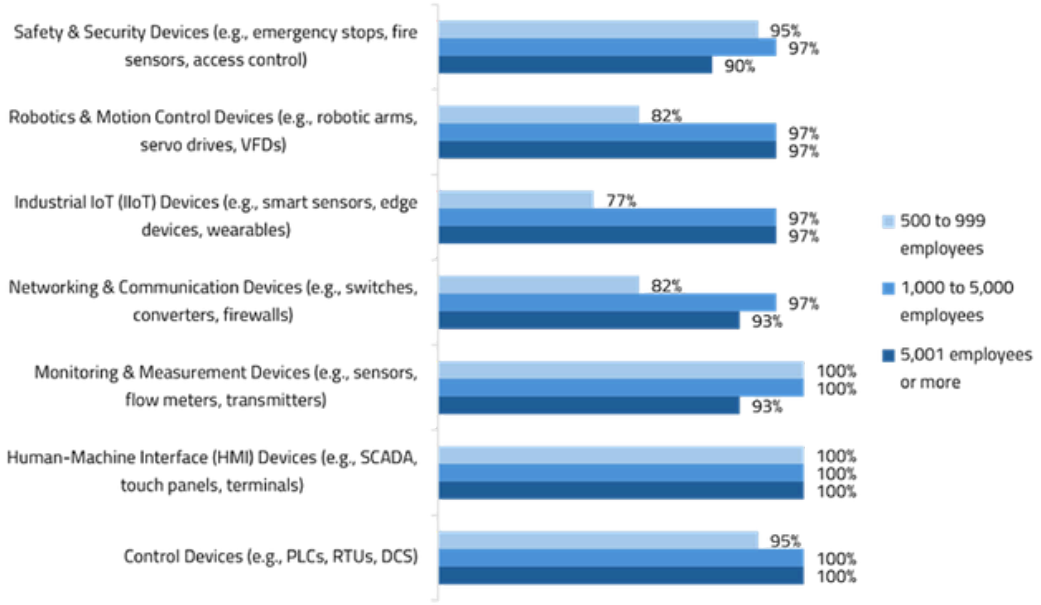
The prominence of "Other" OT solutions in Germany and the US, much higher than elsewhere, reflects these advanced markets' proclivity for innovation and bespoke systems integration.

While core OT systems are universal, the wider ecosystem reveals diverse maturity levels. Germany consistently excels in both breadth and depth of adoption, emphasizing comprehensive OT ecosystem management and innovation appetite. The US shows more variability, shaped by operational stability and organizational hierarchy. Niche solutions mark these markets as pioneers, whereas other regions are yet to fully embrace emerging opportunities—critical insight for strategic technology deployment.

FOUNDATIONAL OT DEVICES: POCKETS OF INNOVATION AMID BROAD ADOPTION

Controldevices(PLCs, RTUs, DCS) dominate with near-universal use(98%),as doHMI, monitoring, networking, and safety/security devices (circa 97–98%). Germany leads, achieving full monitoring/measurement device saturation across all roles.

Differences emerge in robotics and IIoT adoption: Germany (94%) significantly outpaces the US (82%), particularly in smaller firms, highlighting a considerable investment gap. Safety and communication device use is similarly robust in Germany and the US, though slightly lower elsewhere.



The “Other” category of OT devices again confirms Germany and the US as hotbeds for specialized equipment.

This foundational device landscape validates the critical nature of standardized control and monitoring tech in modern OT while underlining uneven distribution of cutting-edge domains like robotics. Germany’s exemplary adoption across device categories reflects strategic prioritization of innovation, with potential lessons for lagging markets seeking competitive agility.

OT DEVICE MANAGEMENT PRACTICES: VULNERABILITY CHECKS LEAD

Vulnerabilityassessments dominate devicemanagement (98%),with fullGerman adoption. Tracking software and firmware changes follow closely and backups—both configuration and documentation—show nuanced regional variation, with mid-level stewardship stronger outside Germany and the US.

98%
Organizations running regular vulnerability checks

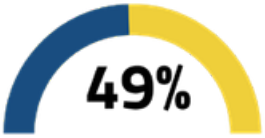
Backup cycles also differ internationally: Germany favors weekly routines for documentation and configuration, the US tends toward monthly, reflecting cultural and operational management styles.

A secure baseline of vulnerability assessment underpins OT device governance worldwide, but backup practices reveal varied operational cultures and maturity. Greater decentralized ownership in some countries may boost resilience and audit readiness, offering a model for organizational governance frameworks.

FREQUENCY PATTERNS: CONTINUOUS VS. SCHEDULED MAINTENANCE

Real-timevulnerability monitoring leadsglobally(49%),strongestin Germany and mid-sized firms. Monthly version tracking dominates in leadership-led contexts, while backup frequency divides weekly (Europe) vs. monthly (US).

49%
Organizations with continuous vulnerability monitoring



The data divide between proactive continuous monitoring and scheduled maintenance reflects operational ownership patterns. Germany's structured backups contrast with American systematic recurrences, suggesting cultural approaches to operational stewardship and process rigor.

OT ENVIRONMENT SIMPLICITY AND STABILITY

Overall,OTlandscapes are perceivedassimpleand stable bymajoritiesacross regions, with Germany recording slightly higher simplicity ratings in device footprint, integration, automation, cybersecurity, data flow, and industry-specific demands.

Most organizations report stable OT environments, particularly large firms (up to 93%), though smaller entities face greater challenges. Stability perception varies by role, with senior management more optimistic than those on the front-line.

This perception aligns with a maturing OT sector balancing complexity with scalability and robustness. However, the disparity in stability experience by role signals the need for strategic alignment between leadership and operations, crucial for risk mitigation and resilience.

CHAPTER II:

OT DISRUPTIONS OUTAGES AND DOWNTIME ACROSS REGIONS

Where resilience is tested by the pressures of modern industry

- Global disruption typology: system downtime, production delays, and communication failures
- Frequency and impact assessment shaped by geography, company size, and managerial tier
- Human error, interoperability gaps, and visibility deficits as root disruption causes
- Operational resilience indicators and leadership-driven mitigation strategies

MAPPING THE FAULT LINES OF INDUSTRIAL CONTINUITY

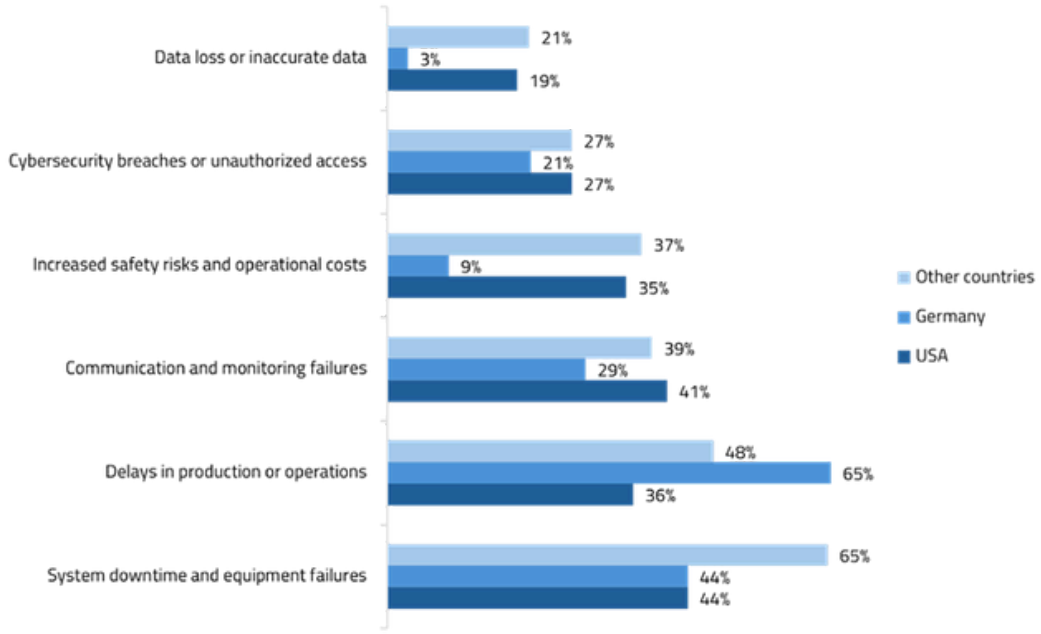
Industrial systems aredesigned for consistency,yet disruptions remain an inevitable part of modern operations. Understanding how and why outages occur—whether through human error, technical failure, or cyber interference—can determine an organization's ability to maintain stability under pressure. This section explores the anatomy of disruption and its ripple effects on productivity, profitability, and cyber resilience.

This chapter provides a comprehensive exploration of operational disruptions within OT environments over the past three years, emphasizing regional and organizational variations. Beyond mere data comparison, it offers analytical insights into the nature, frequency, causes, and business impacts of these disruptions, arming OT professionals with a strategic understanding of current risk landscapes.

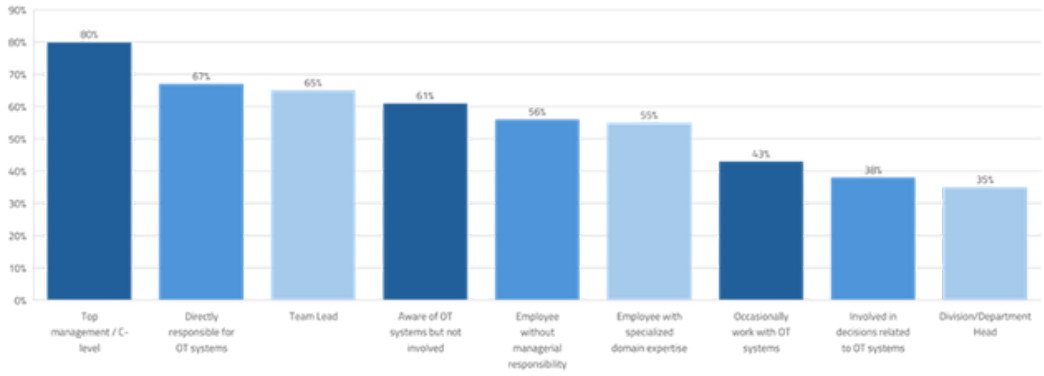
KEY OPERATIONAL DISRUPTIONS IN OT ENVIRONMENTS OVER THE LAST THREE YEARS

System downtimeand equipment failures stand as the leadingdisruptionsglobally, affecting

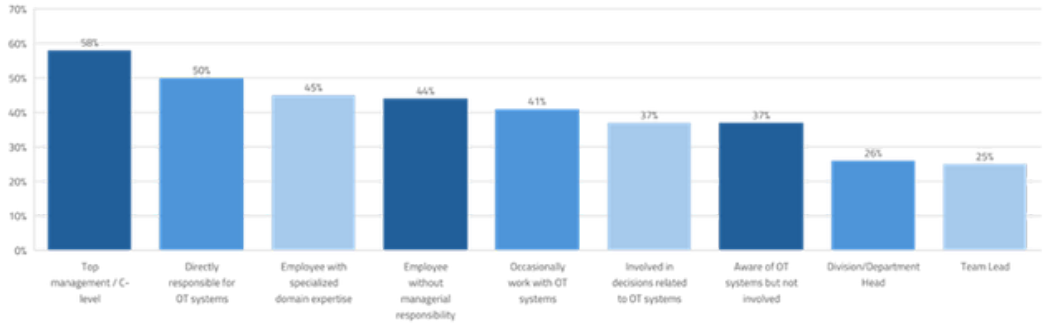
half of all respondents. Disparities emerge, with 44% in the US citing these issues and a higher 62% in other countries.



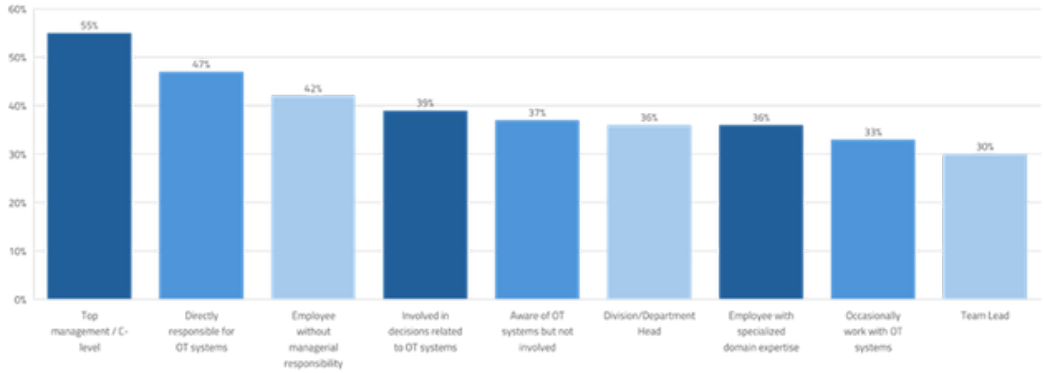
US top management universally (100%) reports experiencing system downtime, contrasting sharply with 30% among division heads. Other countries mirror this pattern (92% top management). Germany presents a nuanced picture: system downtime incidents affect 44% overall but surge to 71% among specialized experts, underscoring their front-line vulnerability.



Meanwhile, production delays dominate in Germany (65%), an issue of lesser prominence in the US (36%) and other regions (49%). Universal acknowledgment by German team leads and domain experts accentuates its operational importance, while in the US, production delays heavily concern senior leaders.



Communication and monitoring failures feature prominently, ranking second in the US (41%) and third in Germany and elsewhere (~30–41%). Role-based perceptions diverge: non-managerial US staff commonly encounter communication issues (56%), whereas top executives in Germany and other countries report these failures more frequently (60% and 58%, respectively).



Data loss or inaccuracies represent the least frequent disruption overall (18%), but remain significant outside Germany (19% US, 24% others).

These data depict a complex disruption landscape tailored by geography and role. German OT environments wrestle mainly with production delays, contrasted by equipment failures elsewhere. Communication challenges disproportionately trouble management in Germany and other countries while affecting front-line US workers. These variances inform targeted disruption management strategies.

FREQUENCY OF OPERATIONAL DISRUPTIONS IN OT ENVIRONMENTS

System downtimeandequipment issues typically occur multiple timesannuallyfor44% globally, soaring to 60% in Germany. Larger firms bear the brunt more often, reflecting complexity-driven exposure. US senior leaders and German team leads report high frequencies, emphasizing their heightened visibility into disruptions. In other countries, mid-level managers and OT-aware personnel register frequent issues.

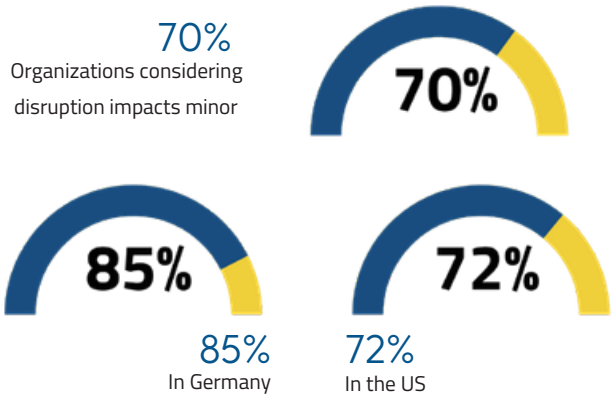
Production delays exhibit lower frequency, primarily annual or less. U.S. large enterprises record highest annual delay rates, German mid-sized companies follow, and large firms elsewhere report occasional more frequent delays.

Communication and monitoring problems occur intermittently (46%), with elevated rates in firms over 1,000 employees. US team leads and OT decision-makers experience these disturbances most. German non-managerial and domain experts, along with top management elsewhere, similarly report frequent occurrences.

The episodic but persistent nature of OT disruptions aligns with organization size and role-specific responsibilities. Larger companies and key operational roles confront disruptions more intensively, reflecting the interplay of operational complexity and managerial accountability.

IMPACT OF OT DISRUPTIONS ON COMPANY

Amajority(70%) considerdisruption impacts minor,particularlyinGermany (85%)and the US (72%). In large US companies, all respondents perceive minor impacts. Similarly, large firms in other countries and smaller German companies predominantly report modest effects.



Role-wise, minor impacts dominate perceptions among US and German division heads and other-country team leads, whereas US non-managers are less likely to see disruptions as minor. Decision-makers in the US and Germany concur with this benign view more than counterparts in other regions.

Moderate impacts are reported by 21%, with higher prevalence among specialized experts, division heads, and US top management. Occasional OT users also denote moderate impacts.

Severe negative effects are infrequent (~7%) and absent in extreme degrees.

The prevailing perception of minor disruption impact denotes operational resilience, though moderate consequences are evident in a meaningful subset, particularly linked to organizational role and maturity. The absence of severe outcomes suggests effective mitigation but continued vigilance.

FACTORS CONTRIBUTING TO OT DISRUPTIONS

Human error ranks as the chief contributor (57%), varying regionally and by company size—highest among smaller firms elsewhere (75%) and large German enterprises (100%). Interoperability deficits (50%) primarily affect large firms and leadership groups, spotlighting system integration challenges.

Visibility deficits in OT assets rank third (42%), more common among smaller companies and recognized by senior leaders and domain experts.

Legacy systems and external attacks are less significant in reported disruption causality.

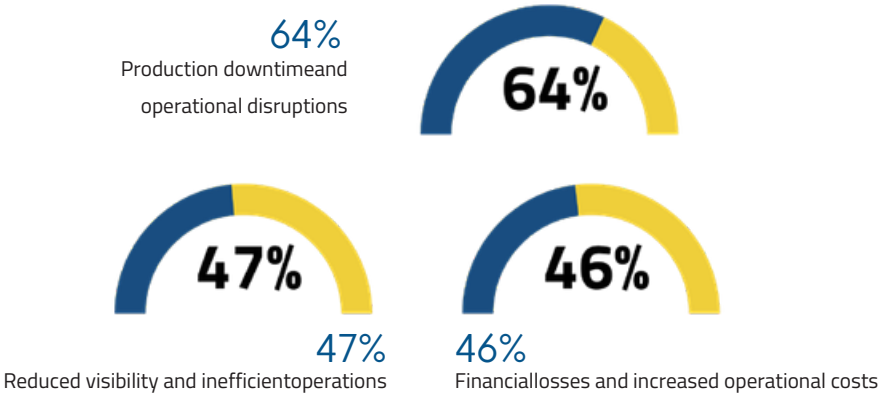
Role variations show leaders emphasize human and interoperability issues, while German team leads identify human error foremost.

OT disruption causality is anchored in human and technical factors, emphasizing the need for comprehensive training, system modernization, and enhanced asset visibility. Role-driven perception differences underscore the alignment necessary between operational execution and strategic oversight.

IMPACT OF OT DISRUPTIONS ON COMPANIES

Production downtime andoperational interruptions impact64%, with greatest effects in

US large enterprises, mid-sized German companies, and smaller firms elsewhere. Visibility challenges affect 47%, notably higher in other countries. Financial losses and operational costs follow closely (46%), with heightened importance in the US.



64%
Production downtimeand operational disruptions

47%
Reduced visibility and inefficientoperations

46%
Financiallosses and increased operational costs

Role-based insights reaffirm that production continuity disturbances gravely concern senior management and domain specialists.

Disruptions principally threaten production and operational efficiency, with financial ramifications more pronounced in specific geographies. Company size and role govern impact perception, guiding prioritization of mitigation efforts.

CHAPTER III:

CYBERSECURITY IN OT NAVIGATING THREATS AND REGULATIONS

Where connected systems demand uncompromising defense

- Cyberincident diversityacrossregions:data breaches,malware, and unauthorized access
- Organizational preparedness and role-based confidence variation in OT defense readiness
- Regulatory frameworks driving adoption: ISO 27001, GDPR, NIS2, and NIST differences
- Evolving strategic focus on IT-OT alignment, network security, and workforce training

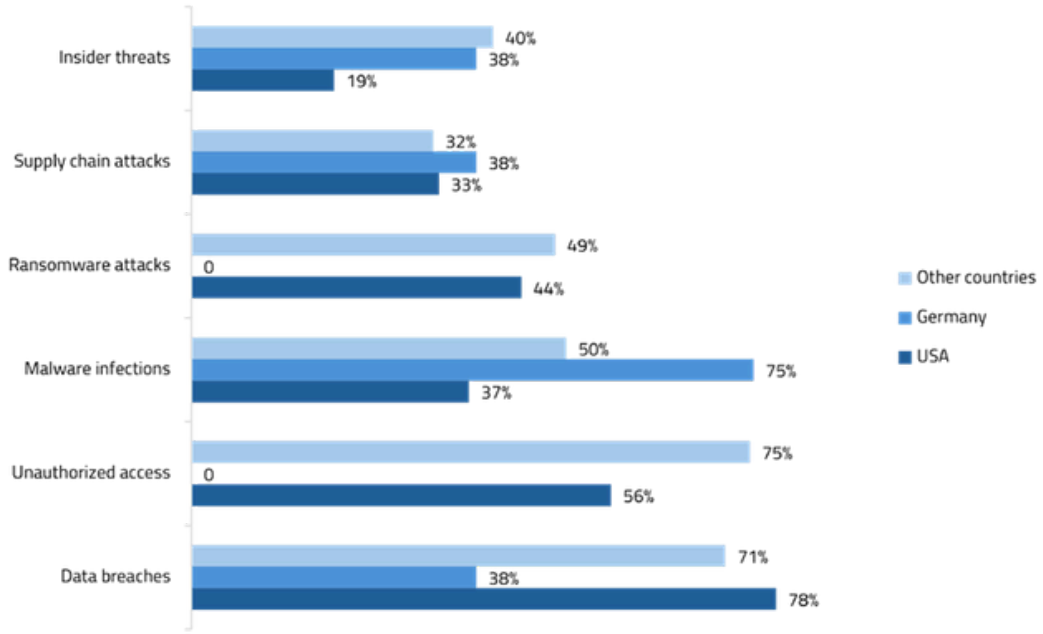
BUILDING RESILIENCE IN AN ERA OF CONVERGENCE

As industrialsystems becomeincreasinglydigitized, the boundaries between IT and OT have all but disappeared, exposing critical infrastructure to evolving threats. Cybersecurity now defines the integrity and reliability of industrial operations. By assessing preparedness, regulatory compliance, and response strategies, this chapter reveals the deep structural shifts required to secure tomorrow's industrial networks.

This chapter provides a comprehensive analysis of cybersecurity challenges and strategies within OT environments. It integrates detailed data on cyber incident types, organizational preparedness, regulatory familiarity, adoption trends, and future strategic plans, enhanced by rich contextual interpretation to guide OT security professionals.

TYPES OF CYBER INCIDENTS FACED IN THE PAST YEAR

Data breachesarethemost frequently encountered cyber incident overall(70%),especially prominent in the US (78%) and other countries (71%). Germany, however, ranks them second (38%), trailing behind malware infections, the most common incident there (75%). Unauthorized access ranks second globally (54%), strongly reported in the US (56%) and other countries (71%), but notably absent in Germany.



Source: Statista 2025

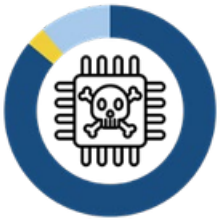
Role influences are strong: US and other-country domain experts uniformly report data breaches (100%), while in Germany, employees without managerial responsibility highlight this issue the most (100%). In terms of company size, the largest US firms (>5,001 employees) report breaches universally, mid-sized German firms lead locally, and large organizations dominate elsewhere.

The cyber threat landscape is diverse across regions. While data breaches and unauthorized access are predominant in the US and other countries, Germany encounters malware as the primary threat. Role and company size modulate exposure and reporting, indicating specialized expertise and infrastructure scale as critical factors in vulnerability.

OVERALL PREPAREDNESS FOR OT CYBERSECURITY THREATS

Most respondents (86%) perceive their companiesas well-prepared for OT cyber threats, with Germany (94%) and other countries (90%) leading, and the US somewhat behind (80%). Large enterprises demonstrate near-universal readiness (up to 100%) across regions, as do organizations with very stable OT environments. Confidence varies by role: US top management shows high preparedness (94%), while only 81% in other countries concur; German and other- country team leads are most optimistic (100%). People directly managing OT systems report lower confidence, especially in the US (63%).

3%
Organizations thatfeel very or rather unprepared for OT cyber threats



86%
Organizations that feel very or rather prepared for OT cyber threats

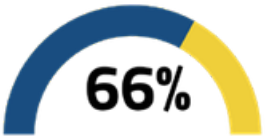
Preparedness correlates strongly with OT environment stability; those in mostly stable contexts feel more confident, particularly outside the US.

Overall cybersecurity readiness is robust but unevenly distributed. Leadership expresses greater confidence than operational staff who experience disruptions firsthand, underlining the need for continuing assurance efforts and capacity building at the operational level.

FAMILIARITY WITH CYBERSECURITY REGULATIONS

Two-thirds of respondents (66%)claim highknowledge of keyregulations (NIS2, NIST, ISO 27001), highest in other countries (74%), then the US (62%), and Germany (59%). Large companies feature greater familiarity, especially in the US (78%) and Germany (64%). Surprisingly, in other countries, small firms (300–499 employees) exhibit the most knowledge (78%). Top executives consistently display the highest awareness across regions; a significant knowledge gap remains among non-managerial staff, notably in the US (23%) and Germany (34%).

66%
Respondents with high knowledge of key cybersecurity regulations



Regulatory knowledge is growing but uneven, concentrated in leadership and large companies. The notable gaps among general staff highlight a need for broader educational efforts to embed compliance culture throughout OT operations.

ADOPTION OF CYBERSECURITY REGULATIONS

ISO27001is themostwidelyadoptedframework (84% overall), particularly strong in the US (92%), where it ranks first. In Germany and other countries, it holds second place behind GDPR. Company size influences adherence: smaller US and German firms (500–999 employees) lead ISO 27001 adoption, while mid-sized companies (1,000–5,000) dominate compliance elsewhere. GDPR enjoys high uptake in Europe (79–83%) and moderate presence in the US (44%), especially in larger firms.

The NIS2 directive ranks third in Germany (43%) and other countries (26%), and fourth in the US. Conversely, the NIST Cybersecurity Framework is more prominent in the US, ranking third (20%) but less so in Europe.

Regional regulatory preferences reflect geographic emphasis: the US favors ISO 27001 and NIST; Europe prioritizes GDPR and shows growing NIS2 traction. These differences inform compliance strategies and resource allocation.

IMPACT OF CYBERSECURITY REGULATIONS ON OT SECURITY

Regulationsare driving changesin security audits,incidentresponse,and employee training—affecting 79% of respondents. The impact is strongest in other countries (82%), with Germany (80%) and the US (76%) close behind. Large companies (>5,001 employees) lead these efforts, especially in the US (86%) and other countries (97%). Germany's mid-sized firms show strong uptake (86%).

79%

Strengthening security audits, incident response, and employee training

Regional priorities vary: Germany focuses on aligning IT and OT security strategies (83%, 91% large firms), the US emphasizes investing in cybersecurity solutions and governance (78%, 84% large firms), and other countries target audits and training (82%) and IT/OT alignment (78%).

Cybersecurity regulations shape OT security approaches with distinct regional lenses—strategic alignment in Germany, technical investments in the US, and procedural strengthening elsewhere—tailored by company size and maturity.

STRATEGIES IMPLEMENTED TO IMPROVE OT ENVIRONMENTS

Network andaccess security arethetopcurrentpriorities (72%), leadingin theUS(75%),secondin Germany (78%), and third in other countries (65%). Large firms spearhead adoption everywhere. Germany prioritizes policies and process efficiency (78%), underscoring organizational rigor. Other countries emphasize supply chain and external security (74%), reflecting broader risk awareness. The US focuses primarily on technical controls.

While network/security defense dominates, regional emphases diverge between procedural discipline, technology, and external risk management. Company size remains a key driver in strategy uptake.

PLANNED STRATEGIES FOR THE NEXT 3 YEARS TO IMPROVE OT ENVIRONMENTS

Future priorities vary: adopting new OTtechnologiesleadsin Germany (44%) and other countries (38%), but is less emphasized in the US (24%). Modernizing legacy systems is more prevalent outside Germany and the US but sees strong niche support from German team leads and division heads.

Cybersecurity training and IT-OT collaboration are planned by about a quarter of respondents, with Germany leading role-specific interest. Supply chain security also gains attention, especially among German team leads and occasional OT users.

A notable US segment (26%) indicates no plans for additional strategies, contrasting with lower percentages elsewhere.

Planned investments reflect varied regional readiness and strategic preferences. Germany's active modernization and collaboration plans contrast with more cautious US postures. Enhancing training and supply chain security remains globally relevant.

CHAPTER IV:

OT DEVELOPMENT TECHNOLOGY INVESTMENT AND INNOVATION DRIVERS

Where tomorrow's factories are built through today's innovation

- Planned adoption priorities:predictive maintenance, digital twins, AI, and 5G integration
- Regional technology trajectories shaping future OT competitiveness and modernization
- Emerging trends: IIoT expansion, IT-OT convergence, and automation dominance in Germany
- Strategic innovation pathways balancing cybersecurity, efficiency, and digital integration

HARNESSING EMERGING TECHNOLOGIES FOR COMPETITIVE AGILITY

The nextphase ofindustrial advancement is beingshaped byinvestmentsin transformative technologies. From AI-assisted analytics to digital twins and edge computing, the innovations redefining production environments are not just enhancing operations—they are rewriting industrial strategy itself. This chapter focuses on the technologies and innovation patterns that will define the factories of the future.

This chapter offers an in-depth comparative analysis of planned advanced technologies and emerging trends slated to influence operational technology (OT) environments globally over the next three years. Drawing on extensive data across regions and organization roles, it distills strategic priorities and contextualizes technological adoption trajectories within evolving industrial landscapes.

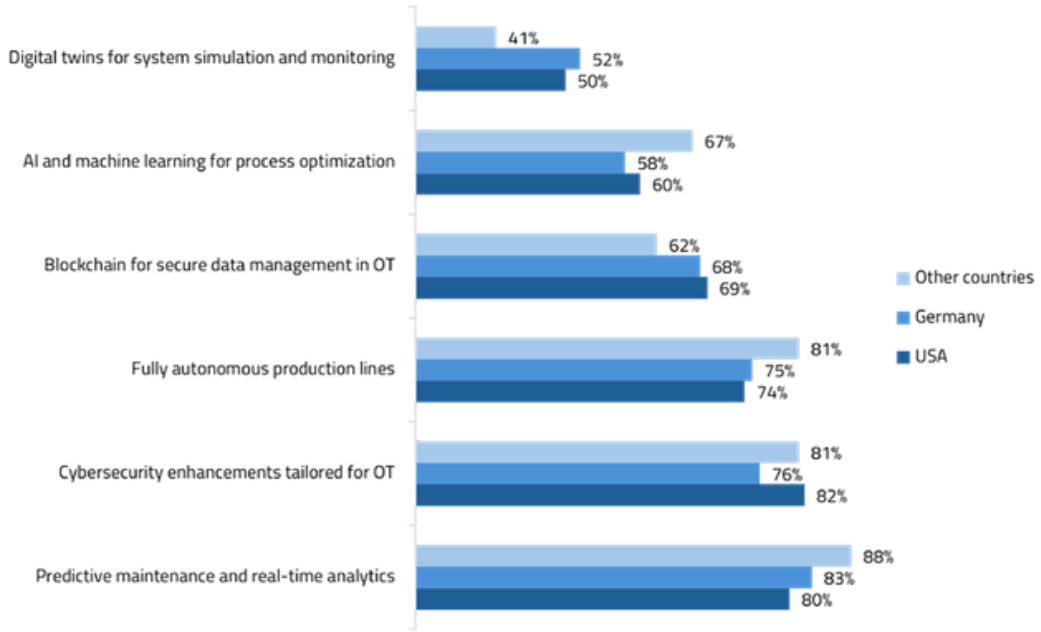
PLANNED ADVANCED TECHNOLOGIES IN OT ENVIRONMENTS OVER THE NEXT 3 YEARS

Predictive maintenance andreal-time analytics command the highestplanned adoption rates, embraced by 88% of respondents in other countries and 83% in Germany. In the US, this ranks second (80%), edged out narrowly by regionally prioritized cybersecurity enhancements (82%), which surpass Germany by six percentage points. This highlights nuanced regional prioritization balancing operational efficiency with security imperatives.

Fully autonomous production lines garner robust interest, with 81% adoption plans in other countries, followed by 75% in Germany and 74% in the US. Digital twins for system simulation and monitoring show pronounced regional divergence: Germany (52%) and the US (50%) outpace other countries (41%) by a notable margin—demonstrating concentrated investment in digital replication technologies within mature markets.

Connectivity advances present the largest regional split: 50% of US respondents plan on leveraging 5G and edge computing to bolster OT connectivity, compared with 40% in Germany and a mere 36% elsewhere. Blockchain for secure OT data management follows, with the US (69%) and Germany (68%) ahead of other countries (62%), signaling clear regional preferences toward data integrity frameworks.

AI and machine learning initiatives favor other countries (65%) slightly over the US (60%) and Germany (58%), indicating a strategic emphasis on process optimization within those regions, contrasting with heightened security and connectivity focus in the US and Germany.



Source: Statista 2025

This technology outlook reveals distinct regional emphases: Germany and the US invest more intensely in security, connectivity, and digital twins, underscoring maturity in risk management and system replication capabilities. Other countries prioritize AI-driven optimization and predictive analytics, reflecting operational efficiency imperatives. These divergences inform tailored technology deployment and innovation strategies aligned with market and industrial maturation levels.

EMERGING TRENDS EXPECTED TO IMPACT OT MANUFACTURING OVER THE NEXT 3 YEARS

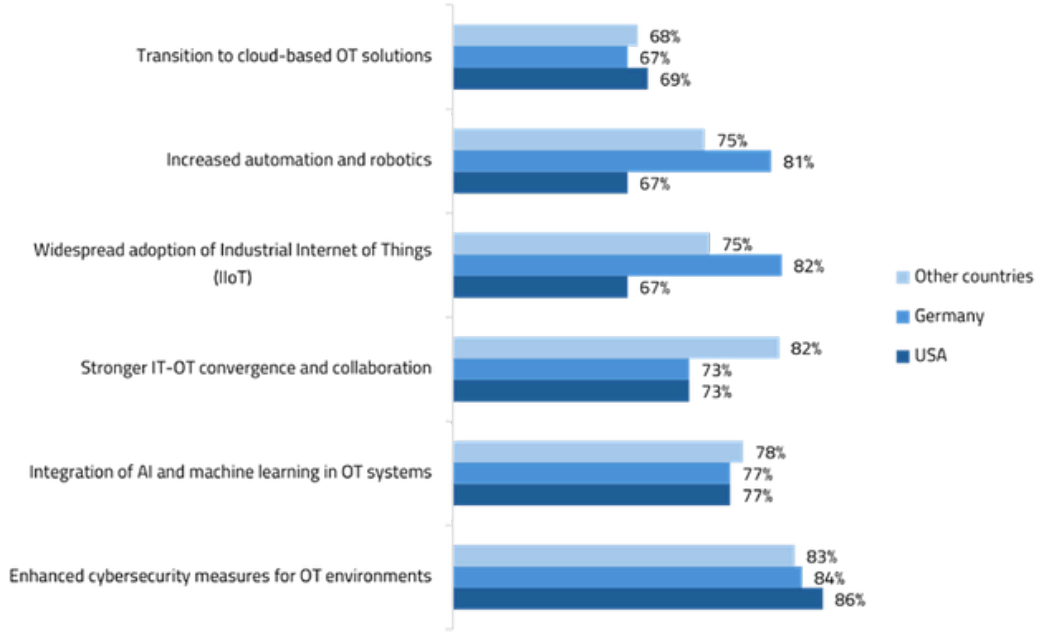
Enhancedcybersecuritymeasures topthe listof influentialOTtrends,anticipated by86% of US respondents, 84% in Germany, and 83% in other countries—an unequivocal focal point across geographies.

The Industrial Internet of Things (IIoT) exhibits substantial planned uptake, notably in Germany (82%), outstripping the US (67%) and other regions (75%) by a significant margin. Similarly, automation and robotics adoption intentions skew higher in Germany (81%) compared to 74% and 67% in other countries and the US, respectively, cementing Germany's role as a leader in process mechanization.

AI and machine learning receive equal expected emphasis (77%) across all regions, though Germany displays wide role-specific variation, from 33% uptake among team leads to 92% among division heads, highlighting internal maturity gaps.

Stronger IT-OT convergence and collaboration is particularly anticipated in other countries (81%) relative to the US and Germany (73% each), indicating differing integration priorities.

Digital twin expansion for predictive maintenance shows relatively balanced regional projections: 51% (US), 48% (other countries), 47% (Germany), indicating broad recognition of its utility despite varied investment pacing.



Source: Statista 2025

The emerging trend landscape portrays cybersecurity, IIoT, and automation as universal priorities with stable cross-regional support, while AI, IT-OT convergence, and digital twins are developing as critical complementary technologies. Regional distinctions reflect maturity, resource allocation, and strategic focus variations. Germany's automation prominence and internal engagement disparities suggest opportunities for targeted capacity building. The pronounced emphasis on collaboration outside Germany and the US signals a growing integration imperative.

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