TATA CONSULTANCY SERVICES

TATA

Future-Ready Manufacturing

TCS Cyber Threat Landscape Report 2026

Foreword

Anupam Singhal
President, Manufacturing,
Tata Consultancy Services

For most people, manufacturing is not something they think about every day. It shows up in simpler ways—in the car that starts every morning, the flight that takes off on time, and the products we rely on without thinking twice.

Over the last few years, that world has changed significantly. Manufacturing today is far more connected and intelligent than it used to be.

AI is playing a big role in this shift. We are seeing more autonomous, agentic systems that can sense, decide, and act—helping organizations operate with greater speed and precision.

In many conversations with manufacturing leaders, there is a growing recognition that this shift also brings a different kind of exposure—one that is not always visible until it begins to disrupt operations in real and immediate ways.

As enterprises adopt these systems at scale, cybersecurity is no longer something that sits within IT. It is becoming fundamental to operational stability, intellectual property protection, and trust.

We have seen cyber incidents before. That is not new.

What is changing is intent.
And the readiness to react quickly, strongly and without much impact to production.

That shift is also changing how these attacks show up:

- **They are no longer just breaking into systems—they are disrupting operations.**

  Increasingly, the goal is to bring production to a halt and create immediate business impact.

- **They do not stay contained.**

  In a connected manufacturing environment, a single breach can move quickly—across plants, partners, and supply chains—before it is even fully understood.

- **And they are not always forcing their way in anymore.**

  More often, they come in through what is already trusted—through identities and access that are much harder to detect, and even harder to stop.

That is why cyber resilience is no longer a technical priority—it is a business imperative.

At the same time, the technologies shaping this landscape—AI and intelligent systems—also offer the way forward. Used well, they can help organizations anticipate threats earlier, respond faster, and build resilience directly into operations.

This report takes a closer look at how the threat landscape is evolving and where attention must shift.

I invite you to explore these insights and reflect on how your organization can strengthen its approach to cyber resilience.

Executive summary

Manufacturing is entering a new phase of cyber risk—one defined not by isolated security incidents, but by persistent, large-scale digital disruption targeting the foundations of industrial operations. As manufacturing ecosystems become increasingly interconnected through digital platforms, cloud adoption, smart factories, and integrated supply chains, cybersecurity has evolved into a core determinant of operational resilience and business continuity.

The threat landscape observed across 2025 signals a structural shift in adversary behavior. Cybercriminal groups and state-aligned actors are no longer focused solely on data theft or system encryption; instead, they are targeting the operational backbone of manufacturing enterprises. Virtualization infrastructure, enterprise applications, identity systems, and supply chain platforms have emerged as primary entry points, enabling attackers to disrupt production indirectly while maximizing financial and strategic impact.

A defining trend is the industrialization of cybercrime. Threat actors are leveraging automation, AI-assisted reconnaissance, and identity-centric attack models to accelerate compromise timelines and evade traditional defenses. Ransomware operations have evolved into extortion-driven campaigns that prioritize data exfiltration and operational leverage over encryption alone. At the same time, phishing and social engineering techniques—enhanced through AI-generated content and impersonation—are increasingly bypassing conventional security controls.

The continued convergence of Information Technology (IT) and Operational Technology (OT) environments represents one of the most significant structural risks for manufacturers. Incidents originating in enterprise IT environments are increasingly propagating into production systems, elevating cyber incidents from technical disruptions to safety, financial, and operational crises. This convergence, combined with expanding supplier ecosystems and distributed engineering networks, has transformed cyber risk into a systemic challenge extending beyond organizational boundaries.

Vulnerability exploitation remains the fastest path to compromise, particularly across internet-facing enterprise platforms, remote access infrastructure, and edge technologies supporting modern manufacturing operations. Attackers are prioritizing high-impact vulnerabilities that enable unauthenticated access, rapid lateral movement, and persistent control over critical systems.

Looking toward 2026, the threat environment is expected to intensify as AI-enabled autonomous attack capabilities mature and geopolitical tensions increasingly intersect with industrial cybersecurity. Manufacturing organizations now operate at the crossroads of economic competition, innovation leadership, and national strategic interests, making intellectual property and production capabilities prime targets.

In this environment, cybersecurity must evolve beyond defensive technology implementation into an enterprise-wide resilience strategy. Leading manufacturers are shifting toward identity-first security models, integrated IT–OT protection, continuous threat intelligence, and supply chain risk visibility to reduce systemic exposure.

The organizations best positioned for the future will not be those that attempt to eliminate risk entirely, but those that embed cyber resilience into business strategy—enabling them to anticipate disruption, sustain operations under attack, and protect innovation in an increasingly contested digital economy.

Purpose and scope

In an environment where cyber threats evolve faster than traditional defense models, manufacturing leaders require clarity—not just visibility—into emerging risks. This report provides a structured view of the cyber threat landscape impacting the global manufacturing sector, translating complex threat intelligence into business-relevant insights that support informed decision-making.

Rather than presenting isolated incidents, the analysis highlights patterns shaping adversary behavior, emerging attack pathways, and systemic vulnerabilities created by digital transformation across industrial ecosystems. The objective is to help organizations understand not only what threats exist, but how they translate into operational and strategic risk.

The indicators of compromise (IOCs) and indicators of attack (IOAs) referenced throughout this report are intended as investigative and contextual guidance. Organizations should evaluate these indicators within their own technology environments, operational architectures, and risk tolerance levels before initiating blocking, remediation, or response actions.

This report is designed to support multiple stakeholders across the enterprise, including:

- Executive leaders seeking strategic awareness of cyber risk exposure
- Security teams responsible for detection and response prioritization
- OT and engineering leaders managing operational resilience
- Risk and compliance functions aligning cybersecurity with regulatory expectations

By connecting threat intelligence with manufacturing realities, the report aims to enable proactive defense strategies that strengthen resilience across both IT and operational environments.

Executive snapshot: Top 5 cyber risks for manufacturing leaders in 2026

Operational Disruption at Scale

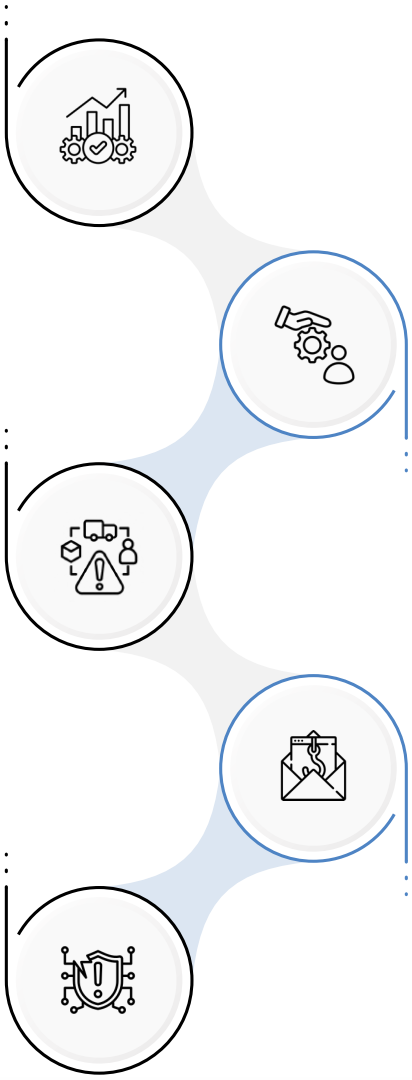
Ransomware campaigns increasingly target virtualization layers and centralized infrastructure, enabling attackers to halt multiple facilities simultaneously and compress recovery timelines.

Supply Chain Cascade Risk

Third-party compromises now propagate across interconnected manufacturing ecosystems, transforming localized breaches into enterprise-wide operational incidents.

IT–OT Convergence Vulnerabilities

Increasing integration between enterprise IT and operational technology systems enables attackers to pivot from corporate networks into production environments, directly impacting safety, uptime, and physical operations.



Identity and Access Exploitation

Credential theft, session hijacking, and abuse of legitimate administrative tools are replacing traditional malware as primary intrusion mechanisms, reducing detection windows.

Phishing and Human-Layer Exploitation

AI-generated phishing, deepfakes, and voice impersonation attacks are bypassing conventional awareness defenses, making employees and partners critical entry points into industrial environments.

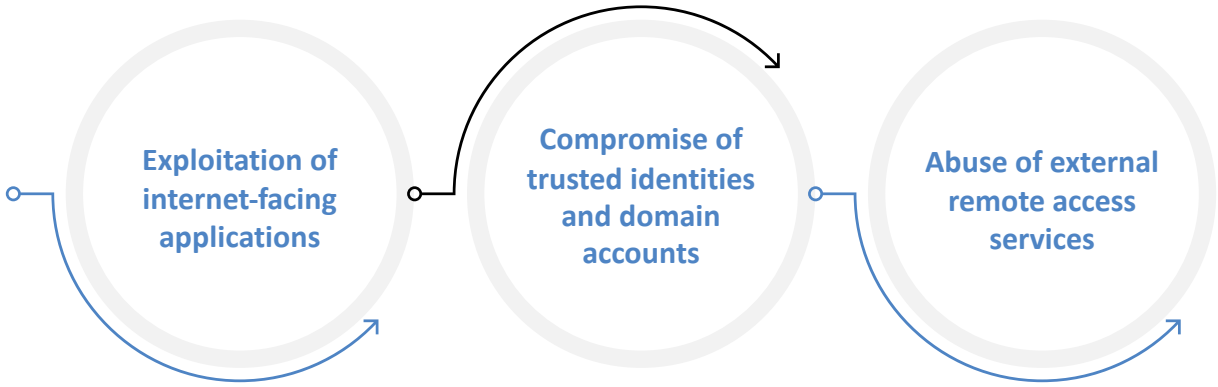
Chapter 1: Manufacturing cyber threat landscape: A system under pressure

The manufacturing sector entered a new phase of cyber risk in 2025 — one shaped not only by increased attack volumes, but by a fundamental shift in how adversaries operate and how industrial environments are increasingly exposed.

Rapid digitalization, Industry 4.0 adoption, and expanding reliance on interconnected operational technologies have transformed manufacturing into one of the most attractive targets for financially motivated cybercrime and state-aligned espionage. As factories, engineering platforms, and supply chains become digitally integrated, the industrial attack surface continues to expand in both scale and complexity.

Manufacturing environments present **uniquely high-impact opportunities for attackers**. Production disruption can halt revenue instantly, cascade across supplier ecosystems, and create immediate operational pressure — conditions that adversaries increasingly exploit through extortion-led campaigns. At the same time, the convergence of IT and OT systems has introduced structural vulnerabilities, where legacy infrastructure, fragmented visibility, and inconsistent patching amplify enterprise-wide exposure.

Manufacturing organizations continued to experience **sustained targeting globally**, reinforcing the sector's position as a primary focus for ransomware operators and advanced threat actors.
The most frequently observed initial access paths included the below:



These entry points highlight a growing shift toward identity-driven and trust-based attacks rather than traditional perimeter intrusion.

Threat actor behavior has evolved significantly. Modern campaigns increasingly combine AI-assisted reconnaissance, credential compromise, and stealthy lateral movement across hybrid IT–OT environments. Ransomware operations now extend beyond encryption, incorporating operational disruption, data theft, and manipulation of industrial workflows to maximize leverage and accelerate payment pressure.

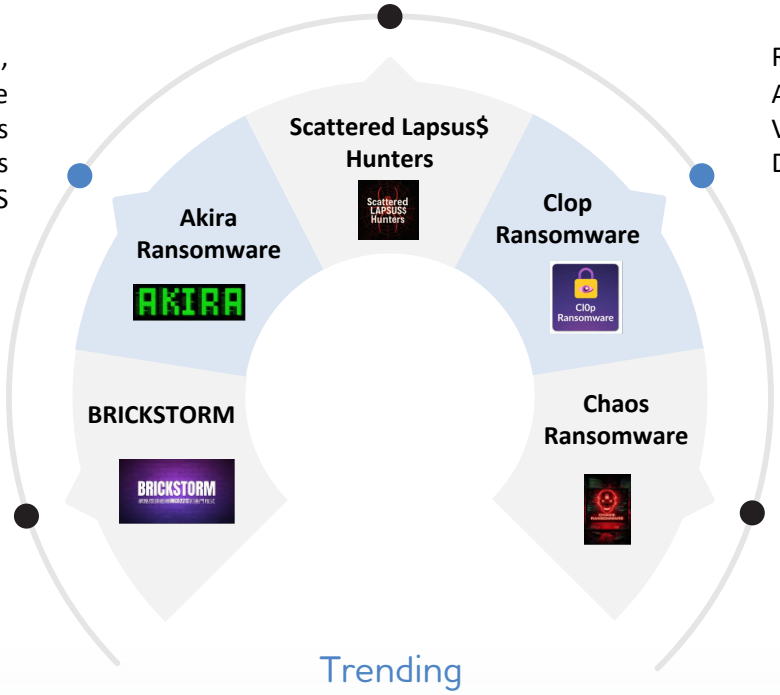
Simultaneously, state-aligned actors have intensified efforts to obtain intellectual property across advanced manufacturing segments such as **robotics, semiconductors, and aerospace**. These campaigns frequently exploit trusted vendor relationships and third-party software dependencies to establish persistent and difficult-to-detect access within enterprise ecosystems.

Trending malware / ransomware

Phishing, Social Engineering, Data Exfiltration, Information Disclosure, RaaS, Financial Gain

Hybrid File Encryption, AD Harvest, Delete Shadow Copies, Writes Memory, Terminates Processes, RaaS

RaaS, Spear Phishing, Application Vulnerabilities, C2C, Deletes Shadow Copies



File & Directory Manipulation, WebShell, Encryption, Command Execution, DoH, Cyber Espionage

RaaS, Social Engineering, RMM tool abuse, data exfiltration, Abuse file sharing software

Trending vulnerabilities

Microsoft SharePoint - Path Traversal

Path Traversal & deserialization of untrusted data, Remote Code Execution, ransomware deployment

Oracle E-Business Suite

Exposed Web Application; improper authentication, Zero-day, RCE; ransomware deployment

SAP NetWeaver

Improper authorization & deserialization of untrusted data; RCE: ransomware deployment

Key malware and vulnerability trends

PAN-OS Web Management Interface

Privilege escalation, OS command injection, POST requests, authentication bypass, RCE

Ivanti Connect Secure (ICS) and Pulse Secure (IPS)

Path traversal, authentication bypass, command injection; unauthorized access, ransomware

Cleo Harmony, VL Trader & Lexicom

OS command injection, Remote Code Execution; ransomware deployment

The global and interconnected nature of manufacturing further amplifies exposure. Organizations depend on distributed suppliers, logistics providers, and contract engineering partners, creating an extended digital ecosystem that adversaries increasingly exploit to bypass hardened enterprise perimeters. The rapid adoption of edge technologies — including smart controllers and remote maintenance platforms — introduces additional vulnerabilities when deployed without strong authentication, segmentation, and monitoring controls.

As a result, manufacturing organizations now operate in a threat environment where operational continuity, workforce safety, and intellectual property protection are simultaneously at risk.

Cyber risk is no longer confined to individual plants or isolated vendors.

It has become systemic, fast-moving, and shaped by shared digital dependencies across the industrial ecosystem.

Chapter 2: Attack innovation: How adversaries rewired their playbook in 2025

The manufacturing sector entered 2025 as the primary arena for cybercriminal monetization and geopolitical cyber activity. Threat actors increasingly shifted from opportunistic attacks toward structured, outcome-driven campaigns designed to maximize operational disruption and financial leverage.

A defining evolution has been the emergence of **extortion-first attack models**. Rather than immediately encrypting systems, adversaries prioritize the silent exfiltration of high-value intellectual property—including proprietary formulas, engineering blueprints, and CAD designs. By delaying visible disruption, attackers maintain persistence while increasing pressure on organizations through targeted data exposure threats.

At the infrastructure layer, adversaries are increasingly targeting **virtualization environments**, particularly ESXi hypervisors and VMware vSphere platforms. Compromising these centralized systems enables attackers to disrupt multiple production workloads simultaneously, amplifying operational and geographic impact while bypassing traditional endpoint defences.

Deepen Desai, Global Head of Cyber, Zscaler

> A Zero Trust platform takes a proactive approach by eliminating implicit trust and reducing the attack surface. Instead of giving employees, contractors, or IoT and OT devices broad access, it grants access only to the specific systems or applications they are authorized to use without exposing the underlying assets. This allows manufacturers to enable secure access to cloud and AI while protecting critical operations.

The expanding digital supply chain has further transformed manufacturing risk exposure. A growing share of incidents now originate from trusted third-party ecosystems, where a single vendor compromise propagates across interconnected enterprises. Threat actors are exploiting software distribution channels and update mechanisms to deploy stealth backdoors such as Sisnitch, enabling long-term access within industrial environments. In parallel, state-aligned groups including APT44 have intensified reconnaissance against OT and industrial control solution providers, seeking strategic entry points into broader manufacturing networks.

The continued convergence of IT and OT systems remains a critical vulnerability multiplier. Adversaries increasingly exploit enterprise network access to pivot into operational environments, targeting engineering workstations and production control systems. Purpose-built malware families such as BustleBerm and Chaya_003 demonstrate a growing capability to directly disrupt industrial operations, halt production processes, and interfere with engineering workflows. Rapid exploitation of edge devices and exposed enterprise applications further accelerates attack propagation across hybrid environments.

A major inflection point in 2025 has been the operationalization of AI-enabled attack methodologies. Threat actors are leveraging Agentic AI and large language models (LLMs) to automate reconnaissance, vulnerability discovery, and command execution at unprecedented speed and scale. Campaigns attributed to groups such as APT28 illustrate how AI-driven tooling enables faster system profiling and precision targeting of high-value industrial assets.

AI-enabled Attack Methodologies

01

Ransomware & Extortion-as-a-Service

Threat actors are shifting from traditional data encryption to **multifaceted extortion** and **extortion-only models**. Instead of encrypting systems, attackers exfiltrate sensitive proprietary data and threaten public disclosure or sale to competitors, reducing the operational complexity of disrupting highly available environments.

02

Exploitation of IT-OT Convergence & Legacy Systems

Attackers are rapidly weaponizing **zero-day and edge-device vulnerabilities**, with new malware families purpose-built to interact with and disrupt ICS/OT environments, including terminating critical engineering and operational processes.

03

GenAI-Enabled Social Engineering

Threat actors are leveraging **GenAI** to deliver highly personalized phishing, deepfake voice and synthetic media attacks, and automated spear-phishing at scale - significantly increasing click-through rates and successful compromises.

04

Supply Chain Compromise

Adversaries are increasingly chaining **zero-day exploits, CI/CD abuse**, and third-party access to enable supply chain compromises, establishing long-term persistence across multiple downstream victims.

05

Identity-Based Attacks & Stealthy Persistence

Attackers are shifting toward **identity-first, stealth-focused operations**, prioritizing credential theft over malware-heavy tactics. Legitimate **remote management tools (RMM)** and built-in system binaries are used to evade detection and minimize forensic traces.

Social engineering has simultaneously entered a new phase of sophistication. AI-generated deepfakes and voice phishing (vishing) techniques are increasingly used to bypass traditional authentication safeguards, including **multi-factor authentication workflows**. Alongside this evolution is a decisive shift toward identity-centric attacks, where credential theft and session hijacking replace malware deployment as the primary intrusion strategy. Infostealers such as Lumma Stealer harvest authentication tokens at scale, while Living-off-the-Land (LotL) techniques leverage legitimate administrative tools—including PowerShell and Visual Studio Code CLI—to maintain persistence while minimizing detection.

Collectively, these developments signal a fundamental transition: cyberattacks against manufacturing are no longer isolated technical events but coordinated campaigns designed to exploit trust, identity, and operational interdependence across digital industrial ecosystems.

Thibault de Assi, Senior Vice President, Head of Digital Connectivity and Power, Digital Industries, Siemens AG

> Cyber disruption in manufacturing has become systemic, deliberate, and increasingly AI-driven. In this environment, cybersecurity is no longer a technical safeguard but a core element of business resilience. By embedding cyber resilience by design and combining it with Industrial AI, Siemens enables manufacturers to protect innovation, sustain operations under attack, and secure long-term competitiveness in an increasingly contested industrial landscape.

Chapter 3: Ransomware and adversary operations: The new industrial threat economy

Manufacturing remained the primary global target for ransomware activity in 2025, driven by its low tolerance for downtime and the high strategic value of industrial intellectual property. However, the defining shift lies in how adversaries now approach the sector - not as opportunistic targets, but as high-leverage environments where operational disruption directly translates into financial and strategic pressure.

This evolution reflects the rise of an industrialized cyber threat economy, where ransomware groups operate with increasing structure, specialization, and scale. Manufacturing environments, with their interconnected systems and supply chain dependencies, offer fertile ground for such targeted operations.

Threat activity in 2025 showed clear signs of this specialization. Adversaries moved beyond uniform attack methods, tailoring campaigns to industrial realities - targeting backup systems to prevent recovery, identity infrastructures to maintain persistence, and supply chain platforms to amplify impact. Increasingly, attacks are designed not just to encrypt, but to disrupt, exfiltrate, and exert sustained pressure.

Campaign momentum intensified through early 2025, with Clop leading large-scale exploitation campaigns and Akira sustaining persistent, high-impact operations across manufacturing networks. The growing diversity and coordination of such groups highlight the maturation of ransomware into a scalable, organized ecosystem.

Together, these trends signal a fundamental shift: ransomware is no longer a peripheral IT risk, but a core business threat, demanding that cybersecurity be embedded as a critical pillar of operational resilience.

Ransomware / Threat Actor	Primary Targets	Exploitation Methods	Threat Actor Profile	Business Impact
Akira (RedBike)	Perimeter infra, backups, virtualization (ESXi, Hyper-V, Nutanix)	VPN & Veeam exploits, lateral movement, credential harvesting, BYOVD, RMM tools	Aggressive, rapid enterprise compromise	Rapid encryption, large-scale operational shutdown
BRICKSTORM (China-nexus)	Manufacturing and defense, virtualization mgmt, domain controllers	Edge device exploits, Brickstorm backdoor, credential harvesting	State-aligned espionage, long-term IP theft	Sustained IP loss, strategic manufacturing risk
Clop	File transfer & data exchange platforms	Mass zero-day exploits, encryption-less extortion, backup deletion	Scalable extortion group	Large-scale data exfiltration, ecosystem disruption
Chaos	Windows, Linux, ESXi, legacy OT	Social engineering, Any Desk/Screen Connect, rapid OT propagation	Adaptable cross-platform, big-game hunting	Operational disruption, destructive impact
Scattered Lapsus$ Hunters (SLH)	Identity systems, enterprise apps, supply chain	Impersonation, identity compromise, RaaS scaling	Hybrid social engineering + ransomware group	Production outages, high-impact operational downtime

Chapter 4: Critical vulnerabilities in focus

Exploited vulnerabilities remained **the primary root cause of cybersecurity incidents in the manufacturing sector throughout 2025**, reinforcing a persistent reality: attackers continue to favour the most direct and scalable paths into enterprise environments. Rather than relying solely on complex intrusion techniques, threat actors are systematically identifying and exploiting weaknesses in internet-facing systems, enterprise platforms, and edge infrastructure to gain initial access.

A significant proportion of high-impact breaches originated from **critical**, **unauthenticated remote code execution (RCE) vulnerabilities**. These vulnerabilities provide adversaries with an immediate entry point - allowing them to establish footholds, escalate privileges, and move laterally across increasingly interconnected IT and OT environments. In many cases, the speed of exploitation has outpaced traditional patching cycles, leaving organizations exposed during critical windows of vulnerability.

This risk is further amplified by the ongoing **expansion of digital ecosystems** within manufacturing. Cloud adoption, remote operations, and deeper supply chain integration have significantly increased the attack surface, while also introducing dependencies on a growing set of enterprise and third-party platforms. As a result, vulnerabilities in core business applications are no longer isolated technical issues - they now translate directly into operational disruption, production downtime, and supply chain risk.

In parallel, attackers are demonstrating greater precision in **targeting widely deployed technologies**, leveraging publicly disclosed vulnerabilities and automated scanning tools to identify and exploit weaknesses at scale. This shift underscores the need for a more proactive and intelligence-driven approach to vulnerability management, especially in environments where operational continuity is critical.

The below mentioned vulnerabilities exemplify the attack patterns and exposure points most frequently observed across global manufacturing environments:

Kunal Pradhan, Global Head – Cybersecurity, Manufacturing, TCS

> Cybersecurity in manufacturing and industrial sectors will be defined less by breaches and more by operational disruption, safety impact, and ecosystem-level risk. Organisations that succeed will be those that embed cybersecurity into engineering discipline, supply-chain governance, and business decision-making - treating it as a foundational component of operational resilience rather than a standalone technology function.

CVSS Score: 9.8

CVE-2025-53770 (ToolShell) Remote Code Execution (SharePoint)

Deserialization flaw in on-prem SharePoint enabling unauthenticated RCE, web shells, and token forgery. Actively exploited by state-aligned actors targeting manufacturing.

Key Takeaway

Collaboration platforms are strategic entry points for stealth-driven attacks.

CVSS Score: 9.8

CVE-2024-55956 (Cleo MFT) Command Injection / Supply Chain

API-level command injection enabling arbitrary commands, payload delivery, and large-scale data exfiltration impacting downstream partners.

Key Takeaway

File transfer platforms are critical supply-chain attack vectors.

CVSS Score: 9.8

CVE-2025-61882 (Oracle E-Business Suite) Remote Code Execution (ERP)

Unauthenticated RCE via BI Publisher HTTP request manipulation enabling persistent ERP compromise.

Key Takeaway

ERP compromise creates enterprise-wide operational and financial risk.

CVSS Score: 9.8

CVE-2025-31324 (SAP NetWeaver) File Upload RCE (ERP)

Unauthenticated file upload enables web shell deployment and full system compromise across SAP environments.

Key Takeaway

Core enterprise platforms remain high-value operational targets.

CVSS Score: 9.0

CVE-2024-9474 (PAN-OS) Command Injection / Perimeter Infrastructure

Command injection combined with auth bypass allows full firewall compromise and covert network visibility.

Key Takeaway

Security infrastructure compromise enables trusted-network exploitation.

CVSS Score: 9.5

CVE-2025-0282 (Ivanti VPN) Zero-Day RCE / Edge Access

Zero-day RCE enabling full VPN appliance compromise and persistent enterprise access by state-sponsored actors.

Key Takeaway

Edge access vulnerabilities offer fastest path to enterprise compromise.

Indranil Sircar, Global CTO, Manufacturing and Mobility, Microsoft

> Manufacturing's cyber risk is no longer about isolated incidents — it is systemic disruption. As IT and OT converge, a breach anywhere can halt production everywhere. The response has to match the scale: verify every identity, every device, every access — before it reaches the systems that keep factories running.

Chapter 5: Manufacturing cyber threat outlook for 2026

Cybercrime is entering an **industrialized phase**, defined by the rapid adoption of AI-driven autonomous capabilities that enable adversaries to conduct reconnaissance, exploitation, and operational planning at machine speed. For manufacturing organizations, this evolution significantly compresses detection and response timelines, transforming cyber incidents from isolated security events **into real-time business disruptions with immediate operational consequences.**

Simultaneously, the continued convergence of Information Technology (IT) and Operational Technology (OT) environments remains the sector's most significant structural vulnerability. A growing majority of observed OT incidents now originate from traditional IT compromises, allowing attackers to pivot from enterprise networks into production systems with increasing efficiency. As manufacturing ecosystems become more connected, cyber risk is increasingly synonymous with operational risk.

Rich Kellen, VP & CISO, International Flavors & Fragrances Inc.

> Cybersecurity is no longer a technical topic - it is a core business risk. At the leadership level, we evaluate cyber risk the same way we assess financial, operational, or safety risk. Security is embedded early in decisions around investments, digital transformation, and supply chain strategy. This ensures we are making informed trade offs and building resilience that supports long term growth and trust.

Dominant threat actor landscape

The 2026 threat environment is shaped by a convergence of financially motivated cybercriminal organizations and strategically driven nation-state actors, each targeting manufacturing for distinct but equally impactful objectives.

01 Financially motivated actors

Ransomware groups such as RansomHub, Clop, and RedBike (Akira) continue to prioritize manufacturing due to the sector's low tolerance for downtime and high-value intellectual property assets. Attackers are increasingly targeting virtualization infrastructure—including VMware ESXi environments to bypass endpoint defenses and disrupt entire production ecosystems simultaneously.

Outlook and recommendation:

Manufacturing downtime has become a predictable monetization strategy for cybercriminal groups. Avoid hypervisor jackpotting by appropriately segmenting the virtualized environment and enforcing controlled privilege access to the management plane.

02 State-sponsored espionage

Nation-state actors are intensifying cyber campaigns aimed at intellectual property theft and strategic industrial intelligence. Groups such as APT45 (North Korea) have targeted automotive manufacturers, while China-linked actors including APT40 and Mustang Panda continue expanding operations across industrial and supply chain ecosystems.

Outlook and recommendation:

Cyber espionage is evolving into a long-term competitive risk rather than a short-term security incident. Enterprises should continuously track their threat profile to effectively address the business risks inherent in this evolving threat context.

03 Destructive operations

The emergence of wiper malware families such as EARLYBLAST and ROTORWIPE signals a shift toward attacks designed for irreversible disruption rather than financial gain. These operations are frequently aligned with geopolitical tensions and increasingly target sectors linked to national economic resilience.

Outlook and recommendation:

Manufacturing industry could be subject to strategic disruption over ransom economics due to the evolving geopolitical situation. Enterprises should reassess backup & recovery strategies, build adequate redundancy for critical business processes and bolster defenses to prevent weaponization of management infrastructure.

Emerging attack patterns impacting manufacturing

01 AI-orchestrated end-to-end campaigns

Threat actors are evolving beyond Ai-assisted phishing toward autonomous attack chains capable of discovering vulnerabilities, adapting exploit strategies dynamically, and even negotiating ransom demands with minimal human intervention.

Outlook & recommendation: Attack velocity will increasingly outpace human-led security operations. Infuse agentic capabilities to augment human analysts to scale and adapt to threat actor's TTPs.

02 Strategic disruption of enterprise software

Enterprise platforms—particularly ERP and production planning systems are emerging as primary attack targets. By compromising the data backbone supporting operational technology, adversaries can halt manufacturing indirectly while maximizing business pressure.

Outlook & recommendation: Data-layer disruption is becoming as damaging as direct OT attacks. Secure development services and adopt secure-by-design approach to facilitate early and deep security integration during the DevOps process

03 Sophisticated cloud-to-edge intrusions

Hybrid cloud adoption has introduced new attack pathways that blur traditional security boundaries. Threat campaigns leveraging malware such as VOIDLINK demonstrate the ability to pivot from compromised cloud workloads into on-premise industrial environments.

Outlook & recommendation: Security perimeters are dissolving into distributed attack surfaces. Build visibility across hybrid, multi-cloud environments and AI workloads to detect cross-domain attacks.

04 Hardware-level sabotage risks

Advanced manufacturing sectors, particularly semiconductor and high-precision engineering environments, face emerging risks involving hardware manipulation and embedded design compromises intended to enable persistent espionage or remote disruption.

Outlook & recommendation: Cybersecurity is expanding beyond software into product integrity and design assurance. Prevent prepositioning attacks by adopting Trusted Execution Environments (TEEs).

Manufacturing in the era of hybrid conflict

Manufacturing organizations are increasingly positioned at the intersection of economic competition, geopolitics, and cyber warfare, making them strategic targets beyond traditional cybercrime motivations.

01 Trade policy and supply chain weaponization

Rising geopolitical tensions are accelerating the weaponization of trade ecosystems. Cyberattacks targeting logistics providers, raw material suppliers, and transportation networks are increasingly used to exert economic pressure across regions.

Outlook and recommendation Supply chain resilience is now a cybersecurity priority mandating focused Third-Party Risk Management (TPRM) strategies.

02 Regional conflict spillovers

Hacktivist groups aligned with geopolitical causes are demonstrating growing capability to leak sensitive engineering data and technical schematics from defense-linked manufacturers as acts of political retaliation.

Outlook and recommendation Reputational and intellectual property risks are expanding alongside geopolitical instability. Threat models must account for and proactively address credible, unconventional destructive attack scenarios.

03 Long-term economic impact

Beyond immediate disruption, sustained intellectual property theft threatens long-term competitiveness and innovation leadership. At the same time, tightening regulatory frameworks—including the EU NIS2 directive and expanding ransomware reporting mandates—are increasing compliance obligations and recovery costs for manufacturers globally.

Outlook and recommendation Cyber resilience is becoming both a regulatory and competitive differentiator necessitating a pre-emptive security approach.

Chapter 6: Cyber resilience as a strategic imperative in manufacturing

The manufacturing sector is no longer confronting isolated cyber incidents; it is operating within a **continuously contested digital environment** where cyber risk directly influences operational continuity, supply chain stability, and long-term competitiveness.

Across the 2025–2026 threat landscape, several defining realities have emerged. Attackers are moving faster, operating at scale, and increasingly leveraging automation and artificial intelligence to compress attack timelines. Ransomware has evolved into operational disruption engineering, identity compromise has overtaken malware as the primary attack vector, and supply chain interconnectivity has transformed single vulnerabilities into ecosystem-wide risk events.

At the same time, the convergence of IT and OT environments has fundamentally altered the nature of manufacturing cybersecurity. Incidents that begin as enterprise IT breaches now routinely propagate into production environments, elevating cybersecurity from a technology concern to a core operational risk. The targeting of virtualization platforms, enterprise applications, and edge infrastructure demonstrates a clear adversary strategy: disrupt manufacturing indirectly by compromising the digital foundations that enable it.

Geopolitical tensions further amplify this risk. Manufacturing organizations increasingly sit at the intersection of economic competition and national strategic interests, making intellectual property, engineering data, and industrial processes high-value targets for both financially motivated groups and state-aligned actors.

In this evolving environment, organizations that treat cybersecurity solely as a technical function risk falling behind adversaries operating with industrialized efficiency and strategic intent. Cyber resilience must therefore evolve into a **business capability embedded across technology, operations, and executive decision-making**.

Looking ahead, leading manufacturers will differentiate themselves not by preventing every attack, but by building adaptive resilience—combining threat intelligence, identity-centric security, IT-OT protection, and supply chain visibility into a unified defense posture. Cybersecurity is no longer only about protecting systems; it is about safeguarding production, innovation, and trust in an increasingly digital industrial economy.

The new cyber reality for manufacturing

01 Cybercrime has industrialized - and manufacturing is its primary battleground

Ransomware and adversary operations have evolved into structured, scalable ecosystems that mirror the efficiency of the industries they target. Manufacturing, with its low tolerance for downtime and high-value IP, has emerged as the most strategically exploited sector - where cyberattacks are designed for maximum operational and financial impact, not just disruption.

02 Vulnerabilities - not sophistication - are driving the majority of breaches

Despite advances in security technologies, most high-impact incidents continue to originate from known, exploitable vulnerabilities in internet-facing and enterprise systems. Attackers are prioritizing speed and scale over complexity, leveraging unpatched exposures to gain rapid access and move laterally across IT and OT environments.

03 Cybersecurity is now a core business resilience function - not just an IT priority

As digital manufacturing ecosystems expand across cloud, supply chains, and connected operations, cyber risk is directly translating into production disruption and revenue impact. Organizations that embed cybersecurity into operational strategy and decision-making will be better positioned to sustain resilience in an increasingly contested environment.

Executive champions

This study was guided and sponsored by the following leaders:

- **Anupam Singhal**, President – Manufacturing, TCS
- **Naresh Mehta**, Global Chief Technology Officer – Manufacturing, TCS
- **Subhash Sakorikar**, Global Head – Manufacturing Industry Excellence, TCS
- **Kunal Pradhan**, Global Head for Cybersecurity, Manufacturing, TCS

Contributors

The executive champions express their appreciation to the following contributors for their expertise and support:

- **Thibault de Assi,**
  SVP, Head of Digital Connectivity and Power, Siemens Digital Industries, Siemens AG
- **Deepen Desai**
  EVP Cybersecurity, Zscaler
- **Rich Kellen**
  VP & CISO, International Flavors & Fragrances Inc.
- **Purna Chander Rao Erabelli**
  Global Head of MDR Practice, TCS

Acknowledgments

The executive champions express their appreciation to the following contributors for their expertise and support:

- **Abhinav Kumar**, Chief Marketing Officer, TCS
- **Vikrant Gaikwad**, Global Head – Industry Marketing Group, TCS
- **Rohaan Mishra**, Global Head of Marketing – Manufacturing, TCS

TCS Additional appreciation to:
Kunal Makhija, Pravir Kumar Rai, Mansha Dhingra, Mrunal Lakal, Kshitish Satapathy, Kartik Korpal, Mayank Sharma, Krishna Tarun Mallareddy, Avneet Kaur Bagga and Venkataraman Kannan.

Notes

Notes

Notes

About the Report

This edition of the Future-Ready Manufacturing TCS Cyber Threat Landscape Report 2026 examines how cyber risk is evolving alongside the rapid digital transformation of manufacturing - shifting from isolated IT incidents to systemic threats impacting production, supply chains, and intellectual property. As factories become hyperconnected and IT–OT environments converge, cybersecurity is emerging as a foundational pillar of operational resilience and business continuity.
The report is grounded in threat intelligence analysis and industry perspectives, bringing together insights from cybersecurity practitioners, manufacturing leaders, and TCS experts. These viewpoints highlight emerging attack patterns, structural vulnerabilities, and the strategic decisions organizations must make to secure increasingly complex industrial ecosystems.
The TCS Manufacturing Cybersecurity Report reflects TCS' perspective on resilient and secure manufacturing - where cybersecurity is embedded by design across enterprise platforms, operational technologies, and digital value chains to enable trusted, future-ready operations.

About Tata Consultancy Services

Tata Consultancy Services (BSE: 532540, NSE: TCS) is the technology partner of choice for industry-leading organizations worldwide. Since its inception in 1968, TCS has upheld the highest standards of innovation, engineering excellence and customer service.
It has set an aspiration to become the world's largest AI-led technology services company and is enabling its clients to transform themselves across the full AI stack, from infrastructure to intelligence. Rooted in the heritage of the Tata Group, TCS is focused on creating long term value for its clients, its investors, its employees, and the community at large. With a highly skilled workforce spread across 55 countries and 202 service delivery centers across the world, the company has been recognized as a top employer in six continents. With the ability to rapidly apply and scale new technologies, the company has built long term partnerships with its clients – helping them emerge as perpetually adaptive enterprises. Many of these relationships have endured into decades and navigated every technology cycle, from mainframes in the 1970s to artificial intelligence today.
TCS sponsors 14 of the world's most prestigious marathons and endurance events, including the TCS New York City Marathon, TCS London Marathon and TCS Sydney Marathon with a focus on promoting health, sustainability, and community empowerment.
TCS generated consolidated revenues of over US $30 billion in the fiscal year ended March 31, 2025. For more information, visit **www.tcs.com**

Follow TCS on LinkedIn | Instagram | YouTube | X