Deloitte.

DSCI
PROMOTING DATA PROTECTION

The state of OT security in India

December 2025

Table of contents

Foreword by DSCI

Vinayak Godse

Chief Executive Officer
Data Security Council
of India (DSCI)

Technology is reshaping India's industrial landscape, further driving the country's digital transformation. What were once isolated Operational Technology (OT) systems are now deeply connected, making them integral to efficiency, but also increasingly exposed to sophisticated cyber-physical threats. Securing these environments has become essential for operational continuity and national resilience.

This joint study by DSCI and Deloitte presents a timely and candid assessment of India's OT security posture. The findings reveal a maturing awareness and efforts being taken, yet highlight that persistent gaps, legacy infrastructure, fragmented governance, IT–OT siloes and supply chain dependencies continue to create systemic vulnerabilities. OT security is no longer a peripheral engineering concern; it is a strategic imperative for the enterprise.

India's regulatory and industrial momentum offers a strong foundation for change. However, sustained progress will require leaders to embed security into design, culture and decision-making. As organisations modernise, resilience must advance in parallel.

Foreword by Deloitte

Gaurav Shukla

Partner and Leader – Cyber
Deloitte South Asia

India’s critical infrastructure is undergoing rapid change. Power grids, oil and gas networks, transport systems, hospitals and advanced manufacturing plants are now deeply connected to the digital world. This forms the backbone of a cyber-physical economy. This integration brings efficiency and innovation but also introduces new risks.

Recent incidents tell the story. From cyberattacks on state power utilities to ransomware shutting down production lines, the threat is real and growing. They underscore a stark reality: Operational Technology (OT) environments are prime targets. Attackers are no longer just targeting IT systems; they are manipulating industrial processes, exploiting legacy protocols and weaponising supply chains to disrupt essential services.

India’s response is gaining momentum. Regulatory mandates from the Central Electricity Authority (CEA), guidance from NCIIPC (National Critical Information Infrastructure Protection Centre) and global standards such as ISA/IEC 62443 show that OT security is finally being treated as critical. However, challenges remain – fragmented IT-OT governance, skill shortages and legacy constraints slow progress while risks accelerate.

This report brings together the insights from CISOs, OT leaders and plant heads across critical sectors. It examines the evolving threat landscape, systemic gaps, and the cultural and technical shifts necessary to protect India’s industrial backbone. It also charts a path where OT security becomes a strategic enabler of trust, continuity and national preparedness.

As India advances towards a digitally empowered economy, protecting critical infrastructure is no longer a matter of operational hygiene – it is a matter of national resilience. The time to act is now, and every stakeholder must come together to make this a priority.

Executive summary

In an era where digitalisation is reshaping India's industrial backbone, Operational Technology (OT) systems, once isolated and proprietary, are now deeply connected, exposed and strategically vital. As factories, power plants and critical infrastructure expand their IT–OT integration, they become more efficient at the cost of becoming increasingly vulnerable if cybersecurity is not thoughtfully designed and implemented. This report, created in collaboration with DSCI and Deloitte India, examines the current state of OT security in India, its pressing risks and the roadmap for building resilience.

India stands at a decisive point. As the country accelerates digital industrialisation, the rise in cyber-physical threats is outpacing the ability to defend them, and the consequences are material. Industrial disruptions caused by OT cyber incidents have resulted in multi-day production stoppages, significant revenue leakage and, in several global cases, share-price impact within hours of breach disclosure. Indian organisations have not been spared; recent incidents in sectors such as power, automotive and pharmaceuticals have revealed how quickly a single compromise can cascade into operational, financial and reputational damage. According to reports from a global Industrial Control System (ICS)/OT security vendor, in Q1 2025, malicious activities were blocked on ~19.1[1] percent of ICS computers in India, with internet-based threats accounting for around 10[2] percent of the malicious actors.

To understand the ground reality of OT security in India, this study was jointly conducted by Deloitte and DSCI, surveying CISOs, OT leaders and security stakeholders across India's critical sectors.

Our methodology combined

- Quantitative surveys across energy, manufacturing, oil and gas, automotive, pharma and transport.
- In-depth interviews with CISOs, plant heads and OT engineers to extract lived challenges and systemic gaps.
- Analysis of industrial threat reports from leading global security firms.

Indian industries recognise the growing threat to OT systems, but preparedness remains inconsistent, fragmented and in many cases, dangerously insufficient.

[1] https://ics-cert.kaspersky.com/publications/reports/

[2] https://ics-cert.kaspersky.com/publications/reports/

The state of OT security in India – Key insights

More than 45%

of the OT security budget is channelised into tool investments such as OT aware firewalls, IDS solutions and network segmentation

25 - 30 years

old legacy systems in OT environments still form the backbone of operations

60%

of the respondents prioritise gaining and improving visibility over the OT assets as the first strategic priority

Average score of 1.75 - 2*

seen as the maturity of OT security controls in the surveyed organizations.

Key thoughts

Quoting a few insights from the discussions with the leaders, such as:

- While there has been an increase in the OT security budgets over the past two years, the funds remain solicited centrally for IT. It is provisioned in a decentralised manner across the OT business units.
- Joint decisions for enterprise-wide OT systems are being made by CISO, CIO and heads of OT as a first step to mutual governance between IT and OT.
- Dependency on OEMs for integration while procuring new security solutions, while withstanding an inherent resistance to external tools for monitoring, is seemingly an increasing challenge faced by OT leaders.
- Performing a targeted OT security gap assessment to understand the plant maturity and existing security controls has helped more than 60 percent of the respondents to know where to channelise investments and the depth.
- A complete convergence for an IT-OT MSSP, while it aids cost optimisation, is not favoured by most of the respondents, taking into consideration safety, operational and the need to address OT-specific security concerns separately.
- The majority of the respondents mentioned that currently, there is an absence of a fixed methodology to calculate the cost of breach in the OT landscape.

*On a scale of 1-5, representing the CMMI Index. 1 representing 'Initial' and 5 representing 'Optimizing'

Why OT security matters now

For years, OT teams took comfort in the belief that air-gapped and proprietary systems offered protection against cyber threats. Yet the recent wave of incidents targeting cyber-physical systems has shattered the sense of isolation, replacing it with a new reality where industrial operations are increasingly targeted with consequences that extend far beyond operational halts.

Across sectors, including oil and gas, power utilities, manufacturing and healthcare, the threats seem to have taken a decidedly aggressive tone. DSCI's India Cyber Threat Report 2025 noted that manufacturing is among the top targeted industries in India, with about 6.88[3] percent of malware detections, with various nation-state actors and cyber criminals deploying sector-specific exploitations.

The inherently high-risk nature of industrial operations means that OT security is no longer just about business continuity, but a more imminent matter of national security. India, as one of the world's largest and fastest-growing digital economies, finds itself at the intersection of regional geopolitical tensions that are escalating into cyber threats. The most common attack vectors included ransomware intrusions through remote access services, unauthorised Programmable Logic Controllers (PLCs) reprogramming and exploitation of outdated ICS protocols such as Modbus and DNP3.

The targeting of OT protocols today is neither accidental nor uniform; adversaries deliberately manipulate industry-specific communication standards to interfere with physical processes at their source. While the power sector, which heavily relies on IEC-104 for Supervisory Control and Data Acquisition (SCADA) communications, remains vulnerable to session hijacking and command injection, manufacturing environments using Profinet and Ethernet/IP have been targeted through packet manipulation and Address Resolution Protocol (ARP) spoofing.

One of the most visible examples was the 2023 cyberattack on one of India's premier national healthcare institutions, which crippled hospital operations for days, emphasising how critical-infrastructure attacks can paralyse essential services. Similarly, multiple state-level power utilities have reported attempted intrusions attributed to Advanced Persistent Threat (APT) groups linked to state-sponsored actors, emphasising the geopolitical dimensions of India's OT threat landscape.

India's regulatory environment has begun to respond decisively to the rising threat to industrial control systems and critical infrastructure, with key regulatory and policy mechanisms shaping how organisations must view and manage OT security. At the apex today stands the National Critical Information Infrastructure Protection Centre (NCIIPC), which spans the critical power, energy and oil and gas sectors, and provides guidelines as part of its broader mandate to protect the critical information infrastructure, addressing the IT-OT convergence.

Recognising the centrality of the power sector, the Central Electricity Authority (CEA) has issued mandatory guidelines requiring periodic cyber audits, establishment of dedicated OT Security Operations Centres (SOCs), network segmentation and incident reporting to the Computer Emergency Response Team for the Power Sector (CERT-Trans), thereby effectively operationalising industry practices of IEC 62443 and NIST SP 800-82 principles for the Indian utilities.

Driven by digitisation and increasing connectivity, the once-separate worlds of physical systems and digital networks have quietly converged, transforming OT Security from a niche engineering concern into a strategic imperative. With companies spending to add statistics and a baseline percentage basis, the interviews aim to provide a flavour of OT spending at the start, targeting key security initiatives for the OT environment. The journey of securing OT is likely to witness a pronounced shift in course.

In the face of an ever-rising need to protect industrial systems, the first step in this journey is clear: to understand the evolving threat landscape and assess the current state of OT security.

[3] https://www.dsci.in/resource/content/india-cyber-threat-report-2025

OT myths – ‘Rewiring beliefs: What OT security is…and isn’t

- Our systems are air-gapped, so they cannot be hacked
- Cybersecurity is IT’s responsibility, not operations
- Legacy systems cannot be secured; we just need to replace them
- Compliance equals security
- A cybersecurity breach is an isolated IT incident that does not affect the production environment or compromise the safety of the people within
- Third-party vendors manage their own security; we’d manage access

Current OT landscape - A reality check

The existing IT-OT siloes creates a human firewall and that is one of the primary areas of concerns today', says an OT leader from the energy industry.

Recognising the growing importance of protecting industrial systems and the OT environment is only the first step. The next, and perhaps the most crucial one, is to understand the threat landscape and assess the security controls that can safeguard the once "isolated" OT cyber-physical systems.

Discussions with OT leaders suggest that while awareness around OT security has significantly expanded over the past few years, preparedness remains uneven and fragmented. With increasing IT-OT convergence, attackers can now exploit the often-inadvertent exposure of an OT device insecurely connected to the internet to establish unauthorised access inside the network. From there, they move laterally to target Human Machine Interfaces (HMIs), PLCs and OT communication protocols that remain highly susceptible to compromise.

This situation makes us talk about the elephant in the room: **what is currently attacking OT systems, and how is the threat landscape evolving?**

What keeps OT leaders awake at night?

1. **Malware that can move beyond boundaries:** Unlike traditional IT malware, modern malware strains are designed to move laterally, crossing corporate networks into plant environments. It is not just a fear of malware, but of malware that understands processes.
2. **Operational halts triggered by ransomware:** Extortion-driven campaigns with prominent groups such as LockBit, BlackBasta and state-sponsored groups that can encrypt a single historian or control interface, halting production lines and putting human safety at stake.
3. **Insider threats:** Negligent and malicious insiders present a significant risk in OT settings where production systems are trusted.
4. **IT risks spilling into OT environments:** Misconfigured cloud services, credential reuse or even a compromised vendor account in IT can provide attackers a bridgehead into the OT domain.
5. **Supply chain:** Vulnerabilities inherited from OEM firmware and engineering tool misconfigurations create systemic weaknesses beyond the organisation's control.
6. **Remote access:** Unmonitored vendor connections and remote engineering workstations that serve as a pathway to exploit the cyber-physical systems.
7. **Lack of awareness of evolving cyber-attack techniques:** Underestimating adversary capabilities and limited knowledge of attack paths, including protocol manipulation to supply chain infiltration, resulting in blind spots around attacks.
8. **Absence of an overarching OT cybersecurity guidance:** Operating without an OT-centric cybersecurity policy leaves the engineering, IT and plant operations teams under IT and safety assumptions that do not account for cyber-attack vectors.

As OT leaders tirelessly aim to mitigate these operational risks, they also shoulder a much larger responsibility: protecting the nation's critical infrastructure in an era where warfare has shifted from physical battlegrounds to cyber-essential targeting of infrastructure.

What critical vulnerabilities in the OT environments help materialise these intrusions faster?

- Misconfigured remote access for maintenance or third-party connections
- Insecure communication protocols like Modbus and DNP3 possess meagre ability to authenticate or encrypt traffic
- Legacy systems, including decade-old PLCs and HMIs that were built to operate in isolated environments
- Human error, the weakest link, ranging from unintentional exposure driven by the lack of awareness to deliberate sabotage fuelled by insider intent

Recent studies further indicate that the manufacturing industry faces the highest concentration of devices with Known Error Vulnerabilities (KEVs), with over two-thirds[4] of them being linked to ransomware groups. In parallel, shifting global economic policies and heightened geopolitical tensions also coerce OT leaders to express a lack of confidence in the integrity and availability of their supply chain. Moreover, Advanced Persistent Threat (APT) groups are increasingly probing India's power and oil infrastructure for reconnaissance or potential disruption. These activities point towards a strategic, long-term focus by nation-state actors on critical infrastructure targets.

As attackers continue to adopt strategic and layered approaches, deploying techniques ranging from mobile security breaches and network device compromises to removable storage and insider breaches, security leaders can no longer view OT as a black box that is safely isolated from exposure.

Organisations grapple with reconciling traditional engineering priorities with the emerging cyber imperatives, resulting in an operational landscape where digital transformation has outpaced proactive readiness.

[4] https://claroty.com/blog/clarotys-state-of-cps-security-2025-ot-exposures#:~:text=7%25%20of%20the%20devices%20are,against%20all%20manner%20of%20threat.

Crux of the challenge: Unpacking the key barriers to OT security

'Building OT security-by-design is a key challenge that we foresee with a critical involvement and integration with OEMs' says a senior OT leader in the manufacturing sector.

Over the last decade, critical infrastructure organisations have become acutely aware of the risks targeting industrial control systems. Yet, the question remains - **if we know the risks, why aren't we able to secure our systems?**

Interactions with security leaders and operational teams reveal a shared sentiment that the challenge is no longer the lack of intent, but the weight of systemic and structural barriers. These constraints, rooted in legacy technology, long-standing IT-OT cultural differences and resource-skill limitations, slow progress and hinder OT security maturity from advancing in tandem with digital transformation and increased exposure.

Technical inertia

At the heart of the security challenge lies the technical inertia of decades-old control systems, which were designed for reliability and isolation, rather than cybersecurity. These systems were built to run safely, rather than securely, thereby creating blind spots and exposing industrial environments to vulnerabilities that attackers can easily target.

IT-OT silos

The barrier after that? IT-OT silos and the organisational misalignment.

IT and OT teams often operate with different priorities: IT focuses on data confidentiality, process integrity and application uptime, while OT emphasises safety and operational availability. This divergence has led to fragmented governance, unclear accountability and inconsistent incident response. While it seems complicated to comprehend, 72 percent[5] of the OT attacks originate in an IT environment. Clearly, attackers and threat vectors have overcome the roadblocks related to the perceived isolation of the OT environment, with IT serving as the primary point of entry.

Is a PLC firmware update an engineering task or a security mandate? Today, the answer varies widely across organisations, a reflection of how deeply the IT-OT divide continues to run.

Lack of OT cyber competency and awareness

Despite cyber threats continuing to grow sophisticated, the OT security competency pool remains relatively narrow. Many OT environments lack even dedicated security personnel, often relying on overstretched IT teams with limited operational context or plant engineers with little exposure to cyber risk management. While both expertise exists and thrives in silos, it is an impending necessity to have people who speak both languages seamlessly.

OT security funding gap

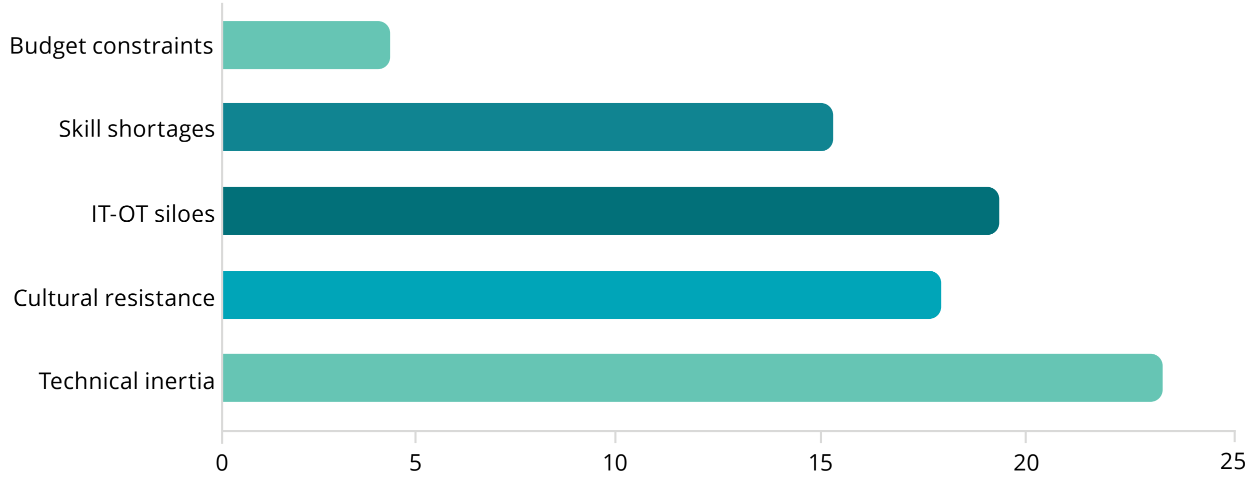
As the OT security funding continues to be embedded within broader IT budgets, the structure creates an inherent competition for resources as IT modernisation, data protection and cloud projects take precedence over OT-specific defences such as network segmentation, passive monitoring and Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS), leading to OT continuing to live in IT's shadow.

[5] https://www.paloaltonetworks.com/resources/research/state-of-ot-security-report

Supply chain

With the industrial ecosystem becoming increasingly connected, vendors, system integrators and third-party manufacturers often now hold remote or privileged access to critical control systems; thus making them a potential conduit for compromise. As trusted software updates and Original Equipment Manufacturer (OEM) firmware upgrades become weaponised to infiltrate operational networks, the result is a web of interdependence where an attacker no longer needs to breach a facility directly; instead, compromising a supplier may be sufficient to gain access.

Figure 1: Key challenges in OT



This chart represents the relative importance of OT security challenges as expressed by participating organisations. Each challenge was ranked by respondents based on its perceived criticality, and scores were assigned using a weighted scale (5 = highest priority, 1 = lowest). The total weighted score for each challenge reflects how consistently and strongly it was prioritised across organisations. Higher scores indicate challenges that surfaced repeatedly as top-tier concerns.

Cultural friction

Beyond systems, skills or budgets, the most persistent barrier lies within the cultural mindset that still views security as an interruption rather than an enabler. “Security slows us down” is a recurring mindset among industrial operators, and the fear of downtime often overrides the recognition of long-term risks and exposures. This culture divide fosters resistance to change, reducing the effectiveness of security policies and leading to inconsistent adoption of controls across sites.

Transitioning from operational continuity to security resilience: Changing the perspective on OT security

> 'We don't touch something that is working – that's a key principle in OT', notes a security head from the automotive industry.

Industrial environments can no longer view OT security as a mere compliance checkbox and a cost centre. Instead, it needs to be positioned as a key driver of business value and an enabler that puts organisations at the forefront of trust, reputation and continuity.

Secure and resilient OT systems enable predictable production, minimise downtime and protect brand reputation, all of which directly contribute to the bottom line. In today's interconnected paradigm, OT cyber resilience becomes a strategic infrastructure rather than just "engineering hygiene".

Are we saying that there seems to be a visible correlation between an organisation's ability to hold ground during an attack and its share values in the market? The answer would be a yes faster than a malware strain can move laterally across an OT network.

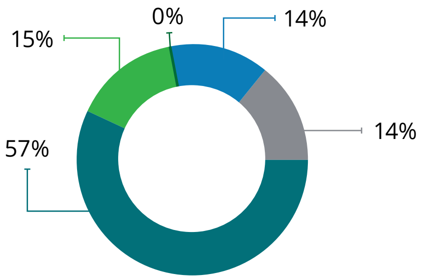
Across India and globally, recent OT cyber incidents in sectors such as automotive, energy, technology, media and telecom have demonstrated that the blast radius of an attack extends far beyond operational downtime. Production halts have led to multi-million-dollar losses, immediate dips in share value and shaken investor confidence. Furthermore, ransomware-induced shutdowns and OT system compromises have delayed critical component deliveries, triggered contractual penalties and strained downstream supply chains, resulting in severe contract attritions and revenue loss. This incident demonstrates that an OT security breach is not simply "OT downtime," but a direct threat to shareholder value, operational continuity and investor confidence that has a much wider blast radius beyond the plant floors.

OT incident response

Today, OT security does not solely sit with engineering, plant operations or IT; it spans all three. The traditional mindset of "IT will handle the cybersecurity; operations will run the equipment" is no longer fit for purpose. As attacks and attackers become smarter, there is only one message to be endorsed by OT leaders today: OT security is not just someone else's problem. A production incident caused by an OT breach is just as much a business issue as it is a reputational and, in some cases, a board-level issue.

If OT resilience defines business continuity, the next question every leader must ask is simple: Are our investments keeping pace with our risks?

Figure 2: Decision-making patterns in OT security spending



🟦 IT team	🟦 Mutual signoff	🟩 OT decides and IT influences
▨ IT decides, OT influences	🟩 OT team	

Trends and patterns in OT cyber investments today

There is little doubt that as awareness of OT risks has evolved into board-level urgency, the investment narrative around industrial cybersecurity has undergone a fundamental shift. The once reactive response to incidents is now evolving into a structured, risk-based programme focused on building resilience, visibility and control.

Across industries, investments in OT security are accelerating, with organisations considering cybersecurity initiatives to protect their OT environment as an essential actionable step. The spending distribution and intent reveal a more nuanced story: a balance between safeguarding legacy systems and preparing for a future defined by convergence and regulatory accountability.

So, where is the money being invested in OT security today?

The investment landscape today reflects a clear pattern that organisations are directing funds toward areas that deliver immediate visibility and risk reduction. A recent study further showed an 18 percent[6] increase in organisations possessing threat intelligence solutions, alongside segmentation, continuous asset discovery and inventory management becoming foundational. Many organisations admit that they still lack a complete view of all connected devices across plants and facilities. A recent report by a global OT/ICS security firm found that over 40 percent[7] of organisations have OT assets insecurely connected to the internet, accentuating why asset visibility remains the starting point for any serious OT security programme.

Complementing these efforts are renewed investments in protocol-aware IDS/IPS, vulnerability management and secure backup and recovery mechanisms, which are being seen as essential to withstand ransomware and destructive attacks that have plagued industrial operations in recent years.

A consistent theme emerging from stakeholder discussions appears to be the challenge of securing legacy systems that were built for reliability rather than resilience. Today, about 62 percent[8] of organisations contain ICS systems that are 6–10 years old, and now organisations seem to be adopting a new approach in the hood: Protect while you replace.

Rather than waiting for the complete modernisation of systems, investments are being made in compensating controls, such as network zoning and secure remote access, to reduce risk exposure in the near term while gradually upgrading systems.

While technology receives the largest share of investment, the spending composition is slowly shifting. Discussions with CISOs and plant heads indicate that organisations are beginning to realise that technology without people and process is unsustainable. On average, OT security budgets are still nested within broader IT allocations, forcing CISOs to compete for resources against priorities such as digital transformation and data protection. This structure not only limits flexibility but also reflects how OT is still seen as a sub-function rather than a strategic pillar

Clearly, there is a dependent relationship between the current attack landscape and the prioritisation of cyber strategies. What are the other factors driving the momentum for OT investments today?

Regulatory pressure

Draft regulations such as the CEA Cybersecurity Guidelines and the rising adoption of ISA/IEC 62443 assessments are pushing critical infrastructure operators to formalise OT security programs and conduct independent audits.

Customer and market trust

Repeated outages or breaches directly affect brand perception and supply-chain reliability, making resilience a competitive differentiator.

Strategic business value

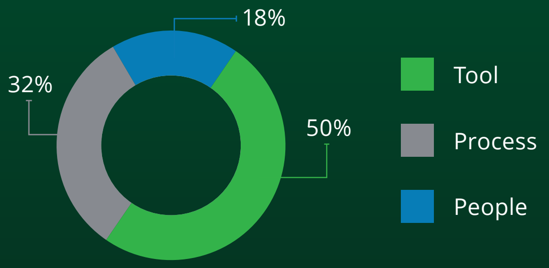
Leading enterprises now treat OT security as an enabler of operational continuity, safety assurance and even investor confidence, recognising that resilience protects valuation as much as uptime.

[6] https://www.fortinet.com/resources/reports/state-ot-cybersecurity

[7] https://claroty.com/resources/reports/state-of-cps-security-ot-exposures-2025

[8] https://www.fortinet.com/resources/reports/state-ot-cybersecurity

Figure 3: Trends in OT security spending



With all said and done, a recurring question from leadership remains: What's the right level for OT investments?

As of today, there's no one-size-fits-all approach. Spending compositions can be calibrated subject to the operational criticality, regulatory requirements and acceptable thresholds. A structured approach to OT investment begins with identifying your high-risk assets and defining the acceptable risk value. Furthermore, continue to prioritise KEVs and internet-facing assets, and then balance spending across tools, people and processes.

How to drive the OT security journey?

> Identifying the crown jewels and calculating the cost of an attack on these assets continue to remain a grey area in the OT environment', explains an OT operations manager from the manufacturing industry.

When conversations around OT security continue to be driven by technology vendors, compliance deadlines and product-led initiatives, they create momentum but rarely sustain the transformation.

As OT environments become increasingly digitised, interconnected and data-driven, securing them is more than just protection. It is about building resilience as a strategic advantage. The organisations that lead the next phase of industrial evolution will be those that can integrate governance, technology and culture into a unified security fabric.

Our discussions with OT security leaders indicate a few core pillars that the future-ready OT security will rest on, forming the blueprint for sustained operational resilience.

1. Governance and accountability

Effective OT security starts with clear ownership.

For decades, security responsibilities in industrial settings have been shared, disputed or ignored between IT, engineering and operations.

This ambiguity is now being replaced by formal governance structures, where OT security is explicitly anchored within enterprise risk management frameworks.

Leading organisations are:

- Establishing OT security forums or committees chaired jointly by CISOs, COOs and plant heads.
- Integrating OT metrics into enterprise KPIs, such as the number of unpatched assets, Mean Time to Respond (MTTR) for OT incidents.
- Mapping compliance with frameworks such as ISA/IEC 62443-2-1 and NIST SP 800-82, which provide structured guidance for governance and control implementation.

This governance has proven to be foundational in building security into the industrial operations' structure for years to come.

2. Risk management

Resilience cannot exist without risk intelligence. The road ahead demands that organisations embed risk management as a living process and not a static assessment.

Risk frameworks, including NIST SP 800-30, ISA/IEC 62443-3-3, are being adopted to perform high-level risk assessments, identify critical OT systems with corresponding zones and conduits and delve deeper into detailed risk assessments based on various security levels.

This allows organisations to prioritise remediation not just by vulnerability count, but by impact on safety, uptime and revenue.

3. Cultural shift and human resilience

Technology can be patched, culture cannot.

Sustainable OT security hinges on cultivating a cybersecurity culture, where operators, engineers and executives view cybersecurity as integral to operational excellence.

It starts with acknowledging that IT and OT are no longer separate stakeholders in this journey. While each preaches a different priority, with IT concerned about confidential data breaches and OT losing sleep over safety concerns and operational halts, today's industry needs them to speak a common language. This includes:

- Integrating cybersecurity into safety briefings and operational training.
- Recognising cyber hygiene as part of performance KPIs for plant and maintenance teams.
- Promoting incident reporting to encourage early detection and transparency.

As seen across leading industrial enterprises, cultural resilience amplifies technical resilience. A plant that values reporting anomalies detects intrusions early, often before automation or AI tools can.

4. Technology and tool adoption

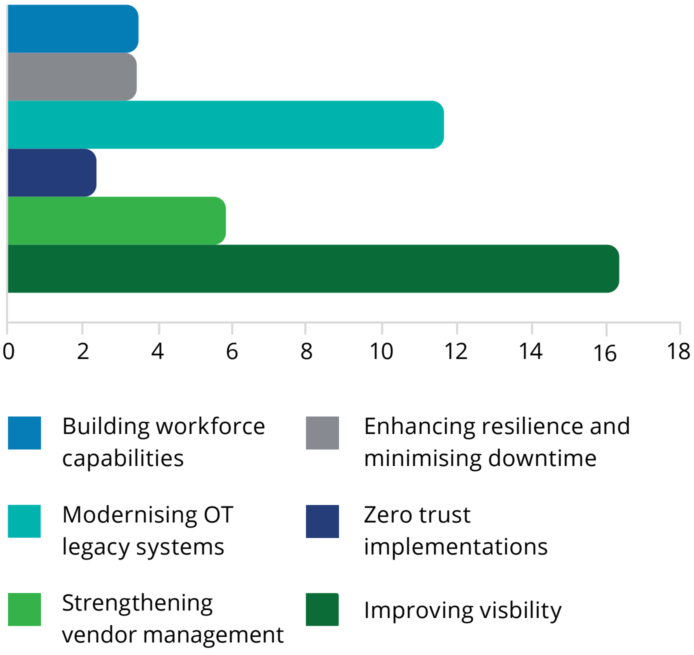
The next decade will see a profound shift from rule- based defence to intelligence-driven, AI-enabled security operations.

Already, AI and ML algorithms are being trained to model normal process behaviour across OT networks, enabling the detection of anomalies invisible to traditional IDS systems.

According to a survey report published by a leading global ICS/OT vendor, over 74 percent[9] of the industrial respondents identified AI-enabled attacks on OT infrastructure as a critical issue, foreseeing a strategic investment in AI-driven monitoring to defend and fortify systems against these threat actors.

This adoption would mark a turning point: Where AI becomes not just a defensive asset but an operational enabler.

Figure 4: Key strategic priorities for the future of OT security



This chart summarises the strategic OT security priorities identified by participating organisations for the next three years. Each respondent selected and ranked their top three priorities, and each rank was assigned a weight. The cumulative weighted score for each strategic initiative reflects both how often it appeared in the top three and how highly it was ranked.

[9] https://www.paloaltonetworks.com/resources/research/state-of-ot-security-report

5. Incident response and operational preparedness

Despite preventive controls, incidents are inevitable, and resilience depends on how quickly organisations respond and recover.

Future OT programmes are embedding industrial Incident Response (IR) playbooks that are distinct from IT IR processes. These define:

- OT-specific containment actions that preserve safety and process integrity.
- Cross-team escalation paths, including IT, OT, vendors and regulators.
- Integration with national CERT-In and NCIIPC reporting protocols and sector regulators such as the Central Electricity Authority (CEA) for utilities.

While traditional IT SOCs cannot fully interpret OT process states and protocol deviations, organisations are now leaning towards OT SOC models that integrate ICS-aware sensors and historian telemetry to provide near real-time visibility of control logic changes and engineering workstation activity. An OT SOC can only be as effective as the intelligence that feeds it, making industrial threat intelligence the next layer of resilience in firms today. Industrial operators are utilising ICS-specific TTPs tied to threat groups and KEV lists, which are mapped to PLC and Remote Terminal Unit (RTU) firmware versions, thereby extending their protection beyond just IT systems.

Conclusion

As threat intelligence sharpens the understanding of adversaries, today, AI becomes the engine to operationalise it. A recent OT security survey by a leading ICS/OT security firm in collaboration with a research organisation in 2024 witnessed about 80 percent[10] of the responders stating that AI-enabled security solutions would be critical for mitigating attacks directed at their OT environments. Yet alongside the promise of AI-enabled detection comes a parallel fear that adversaries will weaponise AI faster than defenders can adopt it, pushing organisations to evaluate AI with caution rather than rush into deployment.

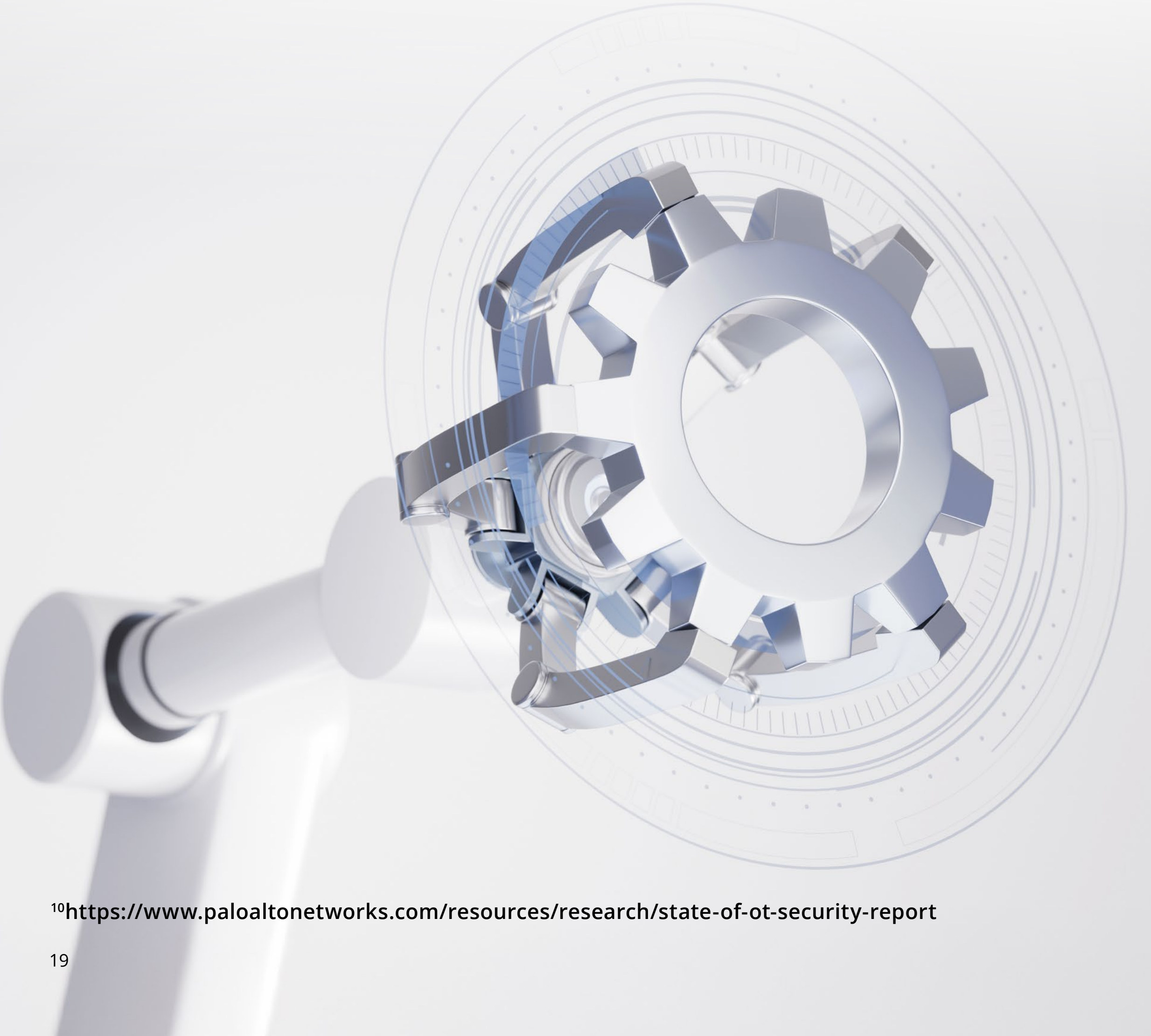
OT security maturity cannot remain static in a threat environment that evolves on a weekly basis. On the other hand, this also does not mean that a Common Vulnerabilities and Exposures (CVE) score of 10 translates to an immediate risk. A factor that has consistently proven essential in considering an OT environment is context. While layers of access control, password limits and patch management may not be the answers to securing OT systems, continual improvement based on context is.

Resilient organisations are adopting Plan–Do–Check–Act (PDCA) models for OT security, mirroring the continuous improvement cycles used in safety and quality management. Each iteration – from post-incident reviews to red-team exercises – feeds lessons back into policy, technology and training. Over time, this creates a self-learning security ecosystem that adapts faster than adversaries.

The organisations that thrive in the industrial landscape of tomorrow will be those that treat OT security not as a project, but as a continuous state of readiness. Governance, risk management, technology, culture and constant learning must converge to form the foundation of this readiness.

The road ahead is one of progressive maturity, where every investment in security fuels not just defence, but business enablement and competitive edge.

Resilience is not built overnight; it is achieved one control, one team and one mindset at a time.



[10] https://www.paloaltonetworks.com/resources/research/state-of-ot-security-report

Way forward

A step in the direction of OT security readiness

Know what you own

Maintain an updated inventory of PLCs, RTUs, HMIs, IEDs, servers, engineering workstations, firmware versions, protocol stacks, remote access paths and safety devices. Map the assets to respective zones and conduits while documenting the OEM support status

Govern who can access what

Enforce strong identification and secure remote access through dedicated jump hosts, session monitoring and approval workflows

Harden the OT components

Require PLCs, RTUs, HMIs, drives and sensors to meet ISO 62443-4-2 component requirements and request OEM Security Level Capability (SLC) documentation and secure development lifecycle evidence

Secure the network

Enforce strict IT-OT segmentation while maintaining plant-wide zoning and controlled conduits

Strengthen supply chain and OEM assurance

Evaluate vendors and integrators based on their alignment with ISO 62443-4-1 (secure development) and 62443-4-2 (component security)

Prepare for the worst

Maintain a dedicated OT security incident response plan with defined escalation paths between operations, IT, OEMs, system integration partners and industry regulators

Connect with us

Deloitte

Sathish Gopalaiah
President, Technology & Transformation
Deloitte South Asia
sathishtg@deloitte.com

Gaurav Shukla
Partner and Leader - Cyber
Deloitte South Asia
shuklagaurav@deloitte.com

Ashish Sharma
Partner
Deloitte India
sashish@deloitte.com

Anand Tiwari
Partner
Deloitte India
anandtiwari@deloitte.com

Santosh Jinugu
Partner
Deloitte India
sjinugu@deloitte.com

DSCI

Vinayak Godse
CEO
Data Security Council of India (DSCI)
vinayak.godse@dsci.in

Bhupesh Janoti
Senior Program Manager
Data Security Council of India (DSCI)
bhupesh.janoti@dsci.in

Contributors

Deloitte

Chinkle Umrania

Akshay Chandra

Swetha Kumar

About

Data Security Council of India (DSCI)

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, setup by Nasscom, committed towards making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, CII, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

https://www.dsci.in/

Deloitte Touche Tohmatsu India LLP

Deloitte is one of the world's largest and most diversified professional services organisations, providing assurance and advisory, tax, management consulting, and enterprise risk management services through more than 345,374 professionals in more than 150 countries. Our organisation includes a unique portfolio of competencies integrated in one industry-leading organisation. Deloitte Touche Tohmatsu India LLP (DTTI LLP) is a member firm in India that provides non-audit consulting services. Our experienced professionals deliver seamless, consistent services wherever our clients operate. In India, Deloitte is spread across 12 cities with over 12,000 professionals, who are proficient at delivering the right combination of local insight and international expertise to our clientele drawn from across industry segments.

Deloitte is well-equipped to deliver solutions to the complex challenges faced by organisations across the public and private sectors. Our edge lies in our ability to draw upon a well-equipped global network and teaming this with customised services at a local office. We have been consistently recognised as leaders by Gartner in the Data and Analytics space, as well for Public Cloud Infrastructure Managed and Professional Services and Oracle Clod Application Services.

https://www2.deloitte.com/in/en.html

Disclaimer

The information contained in this report has been obtained or derived from sources believed by DSCI to be reliable. However, DSCI disclaims all warranties as to the accuracy, completeness or adequacy of such information. We shall bear no liability for errors, omissions or inadequacies in the information contained herein, or for interpretations thereof. The material in this publication is copyrighted. You may not distribute, modify, transmit, reuse or use the contents of the report for public or commercial purposes, including the text, images, presentations, etc. without prior consent from DSCI.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of DTTL, its global network of member firms or their related entities is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication.