Deloitte.

Reimagining OT cybersecurity strategy

May 2022

Contents

Introduction

Digital transformation has started making its way well into the energy and industrial sector. Organisations are adopting newer technologies to improve efficiencies, manage supply chains, and enable remote operations. While technology has many merits in improving the time to market, it is also instrumental in achieving the sustainability vision.

According to the US Energy Information Administration (EIA)[1], between 2018 and 2050, energy consumption is expected to increase by 50 percent globally. With the industrial sector* holding the largest share in terms of end-use consumption, tools and technologies (IoT, sensors, and advanced data analytics) have an imperative towards supporting decarbonisation. This makes the technology-led revolution almost inevitable.

However, alongside us observing the transformation, are cyber criminals, threat actors, and state-sponsored hacktivists, who are targeting these sectors and the whole gamut of critical infrastructure. Operational Technologies (OT) have become a lucrative target for state and non-state actors, as attacking them can disrupt operations, damage equipment, affect lives, and stall economies. Hence, protecting these technologies and improving resilience have become a matter of national security and safety.

This POV probes into why organisations need to reimagine and re-strategise cybersecurity considerations for their OT environment as they embark on their journey of digital transformation and the IT–OT integration.

*According to the US Energy Information Administration, the industrial sector includes refining, mining, manufacturing, agriculture, and construction.

Digital transformation of the energy and industrial sector

By 2025, 'smart factories' are likely to be the key driver of competition, highlighted 86 percent manufacturers in the US.[2] (Deloitte Smart Manufacturing 2.0 series)

Digital transformation and Industry 4.0 are no longer seen as merely new buzzwords. They offer immense potential to companies in the industrial and energy sectors. Whether automating the factory floor, monitoring/operating systems remotely, or using predictive insights for maintenance, newer use cases continue to emerge. Technologies, including automation, Internet of Things (IoT), mobility solutions, robotics, and Augmented Reality (AR)/Virtual Reality (VR), are being introduced into factory floors, in the supply chain and industrial processes.

According to a NASSCOM 2021 report[3], 60 percent manufacturing firms in India reported increasing their digital investments, compared with 63 percent globally.

While most organisations continue to invest in point solutions, some are also creating digital twins of their factory environment to bring the cyber and physical worlds together in a more systematic and meaningful way.

The India imperative

The time is relevant and opportune for the manufacturing sector in India, as it rallies from the impact of the pandemic. The sector is expected to drive growth and garner strong focus under the government's 'Make in India' initiative and its various Production-Linked Incentive (PLI) schemes. For example, INR 25,938 crore for the automotive and auto-component sector and INR 76,000 crore for semi-conductors and display manufacturing, amongst many others. These schemes present an opportunity for organisations to scale their operations while leveraging digital transformation to bring in efficiencies.

Even industries such as power, oil and gas, and chemicals are priming to embrace digital solutions. Last year, the Cabinet approved the Revamped Distribution Sector Scheme[4]. The scheme focuses on implementing smart meters, along with promoting the use of Artificial Intelligence (AI), to analyse data, forecast demand, reduce loses, and provide various predictive analysis. The Ministry of Petroleum and Natural Gas, India, published a digitisation roadmap[5] for upstream processes in 2020. The roadmap highlights encouraging results of using technologies such as AI, IoT, and automation in upstream processes.

The overall concept of smart cities requires real-time and remote monitoring of integrated systems, such as water management systems, electricity consumption, urban mobility, and public transport.

These necessitate the opening up and interaction with OT and Industrial Control Systems (ICS).

Digital transformation and the adoption of the latest technologies in the energy and industrial sector (examples)

An **oil and gas** enterprise in 2019 signed MoUs with various start-ups offering solutions such as intelligent automation, industrial AI platform, AR/VR/3D simulation, and Unmanned Aerial Vehicle (UAV).

A moulded glass **manufacturer** in India installed a new glass furnace during the pandemic using technologies such as AR. It also bolstered the infrastructure to enable remote operation of its plant in a week.

In 2022, an Indian telecom company using 5G standalone network did a trial run to integrate **energy utilities**.

In India, a **manufacturer** categorising itself in the SME segment highlights that its Industry 4.0 implementation is more than 60 percent complete.

Source: News articles


PROCESSING.....
PROGRAM RUNNING...
Robotic Arm Perfo
64%
86%
73%
64%

IT-OT convergence – an enabler and enigma

According to Deloitte US' 2022 manufacturing industry outlook[6], more than half of the organisations surveyed plan to enhance data integration for supply-and-demand visibility and planning. Even in India, the pandemic has established the need for end-to-end supply chain visibility, which effectively means integrating data from operational technologies to have a single consolidated view.

For improved outcomes and productivity, data must be harnessed from operational technologies and made available for enterprise usage, connected to enterprise software, and fed into analytics and AI engines.

Similarly, COVID-19 also brought into focus the need for remote operation and maintenance, which necessitates connecting operational and manufacturing systems to the IT network.

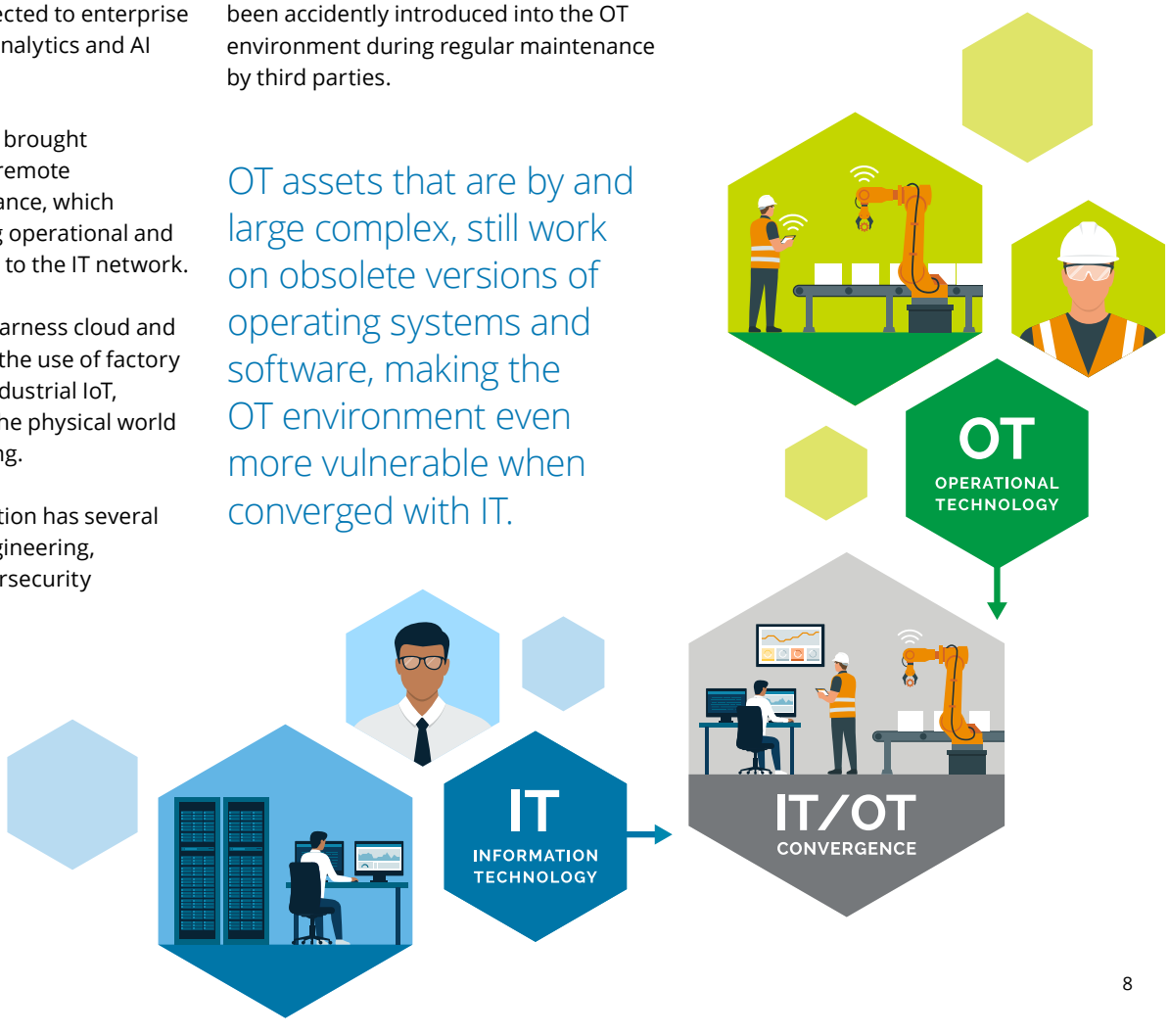
In the overall quest to harness cloud and 5G, and with the rise in the use of factory tablets, robotics, and industrial IoT, convergence between the physical world of OT with IT is increasing.

While the IT–OT integration has several benefits, it brings in engineering, management, and cybersecurity challenges.

If we look at cyber challenges, OT systems have traditionally worked in complete or a partial air gap, isolated from the enterprise network and traffic. The transition from isolated industrial control systems to Industry 4.0, and subsequently to a fully converged environment, allows any existing cyber threats in the IT environment to move laterally into the OT environment. Even a malware from a third party can make its way into OT systems and cause havoc.

Even air gapping as a method has been challenged in the past, and malware has been accidently introduced into the OT environment during regular maintenance by third parties.

OT assets that are by and large complex, still work on obsolete versions of operating systems and software, making the OT environment even more vulnerable when converged with IT.




Warehouse management
Dashboard
Overview
Client order
Stockchecks
Replenishments
Machine State
Monthly Summary
32.04%
PICKS ON GOING
23
Orders by week
25%
Receivals
67%
Machine State
Fine

Cyberattacks and the vulnerabilities of OT systems

According to the Dragos/Ponemon Institute 'State of Industrial Cybersecurity Report 2021'[7], close to two-thirds of those surveyed said they had witnessed an OT/ICS incident in the past two years. A cybersecurity incident's average cost was calculated nearly US$3 million.

There are rising instances of attacks on organisations with OT systems – the ransomware attack on a US pipeline company, the espionage campaign in which organisations in critical infrastructure were targeted for a period of time in a South East Asian country, or the instances of cyberattacks on India's load dispatch units. As the geopolitical environment gets complex, these attacks continue to happen unabated, with several instances of state-sponsored and APT-style attacks.

The ransomware scare has also not spared the industrial sector. Deloitte's recent publication on "Ransomware in critical infrastructure"[9] directs to an analysis that says that ransomware has been observed to be the most prevalent type of attack against industries that have an OT environment. Another recent survey by CrowdStrike[10] brings attention to the rampant ransomware attacks in India – one of the highest in the APAC region.

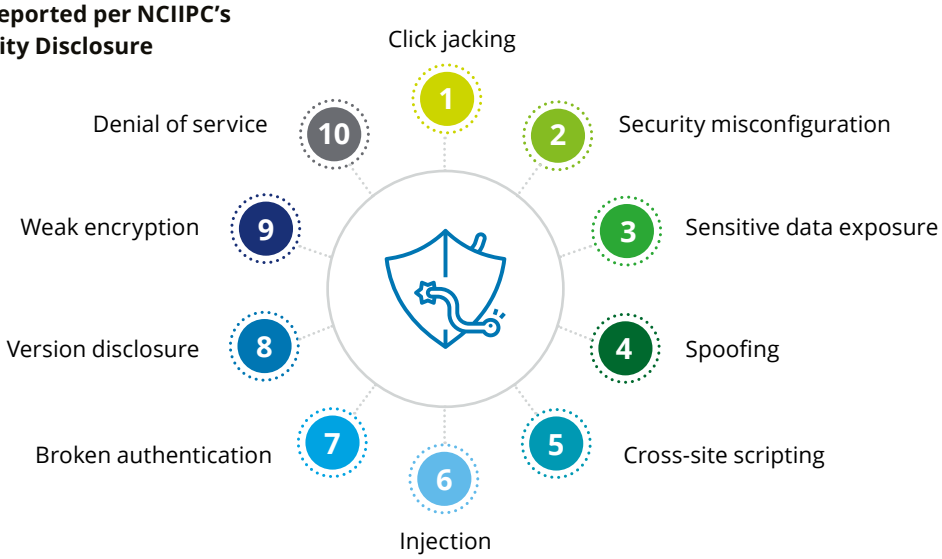
In India, according to NCIIPC's Responsible Vulnerability Disclosure Programme[11], in Q3 2021, 3,913 vulnerabilities were reported in the country's critical information infrastructure; this included click jacking, security misconfiguration, and sensitive data exposure.

On January 11 2022, a joint advisory[8] from CISA, FBI, and NSA was released for critical infrastructure for the US amidst the rising geopolitical tensions. The advisory mentioned the APT-style intrusion campaigns made by state-sponsored groups on the energy sector between 2011 and 2018, and the subsequent exfiltration of data.

Use of legacy systems; lack of proper network segmentation; absence of robust governance, security policies, and monitoring; and unsecure remote access; are leading to increased cyber vulnerabilities.

As the life span of OT assets is high and some vulnerabilities continue due to legacy issues, a different strategy is required to secure and monitor these OT systems.

Top 10 vulnerabilities reported per NCIIPC's Responsible Vulnerability Disclosure Programme in Q3 2021:



Strategising for robust OT security

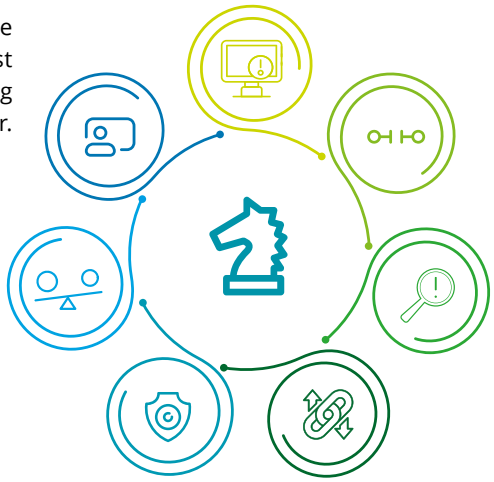
Before we embrace digital transformation within industrial systems, we need to fully evaluate the scope and the need for the IT-OT integration, keeping cyber risks as one of the deciding factors. In the broader Industry 4.0 strategy, an organisation must seek clarity on 'how much is too much.' One can then put a roadmap in place to move from isolated systems to integrated systems, again keeping cybersecurity at its core. The complexities of OT render the traditional IT security strategy ineffective.

Hence, the first step towards the right OT cybersecurity strategy is to acknowledge the following:

The trend of the IT-OT convergence, dissolving air gap, and the rise in attacks (targeted or otherwise)

Irrespective of the industry, the human element is the weakest link. Hence, the focus on training and awareness should be higher.

The fact that air gapping provides a false sense of security, and cybersecurity awareness and measures are equally critical even if OT assets and network are completely isolated



OT security is a cross-functional responsibility. Setting the right governance structure, and establishing roles and responsibilities are important. This helps determine the right balance of risk and reward.

Due to interdependencies building up with hyper-convergence and digitisation, even an attack on enterprise IT can affect operations. Hence, complete visibility and monitoring of devices and network within the IT, OT, and IoT environment, is needed.

As service availability is crucial, a strong focus on cyber resilience and business continuity is needed.

Any attack in the supply chain can laterally move into the OT system. Therefore, security considerations in any external collaboration are must.

Setting the right governance is key

Establishing a governance model is key. It enhances accountability and collaboration amongst the IT security and OT teams, along with balancing risks and rewards. Simple tasks such as system upgrading and patching are complex. They require revisiting the technology stack and necessitating intervention of manufacturing teams.

OT environments and systems have traditionally been under the purview of manufacturing or engineering teams, with the IT function monitoring network at some of the IT-OT interface and laying out protocols/standards for technology use and implementation. As the scope of technology, associated vulnerabilities and threats increase, the governance of OT security needs further thought and elevation at the management and board levels.

Just like IT, OT cybersecurity teams require specialists for governance, risk, and compliance; security design and engineering; monitoring and assessment; and respond and recover. With challenges around talent availability, organisations are also considering managed security service providers to establish their satellite OT security teams.

A joint governance with the senior leadership of IT, security, engineering, and management can provide the appropriate attention and security to OT systems. It can also help better correlate and assess the impact of cyber risks on business operations.

The need for specialised OT cybersecurity teams, mapped to the CISO function, is also emerging. This will encourage better measures, controls, and monitoring.

Best practices and controls to secure the OT environment

- In line with the evolving threat landscape, the Indian government in 2021 released guidelines for cybersecurity in the power sector (see Appendix).
- The joint advisory[8] from CISA, FBI, and NSA for critical infrastructure (amidst the rising state-sponsored attacks) recommends patching systems (amongst other requirements). It also suggests implementing multi-factor authentication (MFA), robust log collection and retention, behavioural detection, and proactive threat hunting, alongside formulating an incident response and resilience plan, and a plan for continuity of operations.

To secure their OT environment, organisations can consider a six-point framework:

In-depth security assessment to establish the security posture

Amidst greenfield or brownfield digital projects, a comprehensive security assessment helps understand security maturity levels and existing gaps. Moreover, it provides visibility on asset inventory across levels – field devices, process controls, supervisory, and enterprise IT network. This helps understand the current security levels and put the right OT security process and roadmap in place.

Security processes, protocols, and controls

Following IEC 62443 standards (Cybersecurity for Industrial Control Systems) across policies, management, industrial IT, products, and components, is important.

Security considerations include, but are not limited to, designing a secured network segmentation model and secured remote access, as well as managing privileged access, data backup, and passive monitoring for visibility of networked assets and activity.[12]

Any digital programme or third-party collaboration must have a "security-by-design" and "resilient-by-design" approach to be able to successfully mitigate risks. For products, systems, and the development lifecycle, third-party assurance certifications complying with standards such as IEC 62443-4 are imperative.

Periodical risk and vulnerability assessments and audits can help take the right step towards bolstering security, while providing the required security assurance.

24x7 monitoring via a robust next-gen IT-OT security operations centre (SOC)/threat intelligence centre

As both the environments integrate, it is pragmatic to have a common IT-OT SOC, using specialised OT security solutions that help in asset identification, visibility, anomaly detection, and monitoring. Having custom OT-specific playbooks, use cases, and a common SOC empowers security teams to effectively join the dots and respond faster to threats.

Incident response and cyber crisis management plan for the OT environment

Formulating a cyber incident response and cyber crisis management plan is imperative. The plan must undergo regular reviews of the board and others. The plan should address various scenarios affecting OT systems, including emerging threats and attacks such as ransomware. Industries should also focus on having table-top exercises for executives to prepare them towards various scenarios.

Awareness and training

Training and awareness is one of the crucial aspects of OT cybersecurity strategy. It helps create an in-house team of OT security specialists (for example, with expertise in PLC testing and infrastructure testing) or provide awareness and hygiene training to employees that operate systems. Training is also important to create a security-first mindset to ensure that cybersecurity remains a key tenet of Industry 4.0 implementation within an organisation. This can also help prevent Shadow IT, which becomes a pain point in the effective management of security.

Red teaming

Red teaming is essential to test resistance and resiliency of OT environments to stay ahead of malicious threat actors. A robust mechanism should also be set in place to incorporate leanings, plug-in gaps, and enhance security.

Conclusion

While the industrial sector was gearing up and strategising for digital transformation, the pandemic provided an opportunity to test the waters, even for the most reluctant organisations. This helped place the spotlight on possibilities and opportunities, and at the same time, brought awareness about various risks. There is, perhaps, no turning back. Driven by the changing business priorities, regulatory environment, and the threat landscape, organisations with OT must look at embracing a cybersecurity strategy that puts OT security into perspective.

The geopolitical environment will continue to rapidly evolve, making the security considerations for OT not only an organisational mandate, but also a country-wide imperative. The road to a safer, secured, and resilient industrial ecosystem must include removing silos, collaborating to synergise intelligence and proactively dealing with syndicated attacks.

There is no better time than now to prioritise and streamline OT cybersecurity.

Endnotes

1. "EIA projects nearly 50% increase in world energy usage by 2050, led by growth in Asia", US Energy Information Administration (EIA) (https://www.eia.gov/todayinenergy/detail.php?id=41433)
2. Smart Manufacturing 2.0 series, Implementing the smart factory - New perspectives for driving value, Deloitte (https://www2.deloitte.com/cn/en/pages/energy-and-resources/articles/implementing-the-smart-factory.html)
3. Reimagining Indian Enterprises' Tech Landscape In A Digital-First World – A New Order Out Of Chaos, NASSCOM analysis (https://nasscom.in/knowledge-center/publications/reimagining-indian-enterprises-tech-landscape-digital-first-world)
4. "Cabinet approves Revamped Distribution Sector Scheme: A Reforms based and Results linked Scheme", Press Information Bureau (https://pib.gov.in/PressReleasePage.aspx?PRID=1731473)
5. Digitalization Roadmap for Indian Exploration and Production (E&P) Industry, Ministry of Petroleum and Natural Gas http://petroleum.nic.in/sites/default/files/Draft_digitalization_roadmap_document.pdf)
6. 2022 manufacturing industry outlook, Deloitte US (https://www2.deloitte.com/us/en/pages/energy-and-resources/articles/manufacturing-industry-outlook.html)
7. 2021 State of Industrial Cybersecurity, Dragos-Ponemon Institute (https://hub.dragos.com/hubfs/Reports/2021-Ponemon-Institute-State-of-Industrial-Cybersecurity-Report.pdf?hsLang=en)
8. Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure, Cybersecurity and Infrastructure Security Agency (CISA) (https://www.cisa.gov/uscert/ncas/alerts/aa22-011a)
9. Ten key questions and actions to tackle ransomware in critical infrastructure, Deloitte (https://www2.deloitte.com/tw/en/pages/risk/articles/ransomware-in-critical-infrastructure-ten-questions.html)
10. Indian businesses hit by more ransomware attacks than Australia, Japan and Singapore reveals new survey, Business Insider (https://www.businessinsider.in/tech/enterprise/news/indian-businesses-hit-by-more-ransomware-attacks-than-australia-japan-and-singapore-reveals-new-survey/articleshow/79279334.cms)
11. Newsletter, October 2021, National Critical Information Infrastructure Protection Centre (NCIIPC) (https://nciipc.gov.in/documents/NCIIPC_Newsletter_Oct21.pdf)
12. Cybersecurity for smart factories, Deloitte and the Manufacturers Alliance for Productivity and Innovation, 2020 (https://www2.deloitte.com/us/en/pages/energy-and-resources/articles/smart-factory-cybersecurity-manufacturing-industry.html)

Appendix

Central Electricity Authority (Cybersecurity in power sector) guidelines, 2021

In line with the evolving threat landscape, the Indian government has also come up with cybersecurity guidelines for the power sector. These guidelines lay emphasis on certain key aspects (amongst others):

- Having an Information Security Division, headed by a CISO
- Receiving ISO/IEC 27001 certification, along with other certifications
- Formulating a cybersecurity policy that should be reviewed annually
- Making cybersecurity issues a part of the board agenda, taken up every quarter
- Identifying and declaring 'critical information infrastructure'
- Defining electronic security perimeter, with conducting vulnerability assessment of access points at least once in six months
- Ensuring round-the-clock monitoring, with adequate resource support
- Devising a cyber risk assessment and mitigation plan, with quarterly reviews
- Phasing out legacy systems
- Conducting security and testing of cyber assets, and external audit of IT and OT systems at least once in six months
- The CISO is expected to report any anomalous activity caused by the sabotage of critical systems within 24 hours of occurrence. For not reporting any identified sabotage, CISO to be held responsible.
- Ensuring cyber supply chain risk management with assurance certification for embedded device security, system security, and security development lifecycle (in line with IEC 62443-4 standards)
- Putting in place cybersecurity incident response and cyber crisis management plans
- Conducting annual cybersecurity training for employees having access to critical systems (either cyber or physical access)
- For IT and OT professionals, providing training to introduce various standards, such as ISO/IEC:15408, ISO/IEC:24748-1, ISO: 27001, ISO: 27002, ISO 27019, IS 16335, and IEC/ISO:62443

Connect with us

Rohit Mahajan
President - Risk Advisory
Deloitte India
rmahajan@deloitte.com

Gaurav Shukla
Partner and Leader,
Cyber, Risk Advisory
shuklagaurav@deloitte.com

Santosh Jinugu
Executive Director,
Risk Advisory
sjinugu@deloitte.com

Contributor

Manishree Bhattacharya

Deloitte.