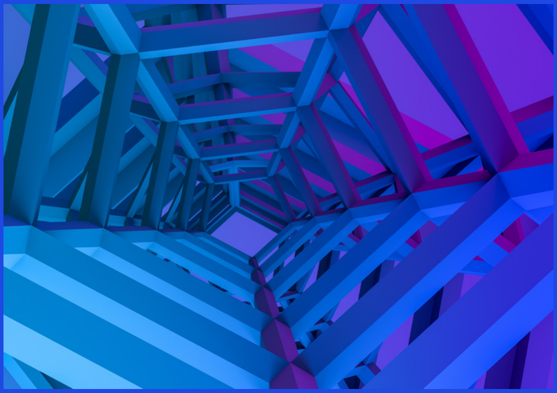
Cybersecurity in the space sector



The role of OT

Setting the stage

To address the fast-paced evolution of the space sector—commercial, civilian, and military—there is a growing imperative for all business leaders to consider the impact of space activities on their industry and organization. The pervasiveness of space-originating data and services in our economy and everyday lives underscores this imperative. Additionally, the potential for conflict in the space domain is on the rise. One of the most prevalent threats is cyberattacks. In our first series on cross-sector implications, we look at cybersecurity considerations in this evolving sector.

In this chapter of the cybersecurity considerations series for the space sector, we address operational technology (OT) in the space sector.

Operational technology in the space sector

Traditionally, information technology (IT) has driven the conversation in cybersecurity, especially in the space industry, with IT teams supporting OT deployment in factories. Today, that is not the case. Increasingly, we are seeing OT generate data that is incorporated into digital initiatives to improve decision-making. The insights derived from OT are catching the eye of key stakeholders within the enterprise, which in response is turning the heads of top executives.

With a shift in focus to OT, the question for many companies becomes, how do we use operational data in new ways to provide operational visibility, cost reduction, and factory performance? To answer that, we first must address the lack of strategic leadership buy-in, roadmap, or even structured collaboration (Lang, 2022a) between the IT and OT initiatives. Very few organizations have found an answer to the IT/OT challenges and built a mature framework.

Within the space sector, rocket and satellite manufacturing are seeing a greater shift in focus and the most impact in OT, providing operational visibility to the broader organization, primarily as new pressures arise and existing forces shift customer demand, automation, OT skill set, economic uncertainties, and more. The risks of simply writing-off OT strategy within rocket and satellite manufacturing are high. Any downtime or unplanned outage from a breach can cost the manufacturer money, reputation, and even safety concerns. Unlike previously, when these breaches affected mostly the IT environment (e.g., the HR system going down), it is now targeting the OT environment (e.g., the ability to manufacture parts is delayed).

Even though IT and OT are working together, combining the two in the short term may not be the simple answer. Through extensive analysis, it has been hypothesized that connecting OT air-gapped networks to the IT environment could introduce multiple cybersecurity risks since OT systems tend to be slower in the patch cycle due to a lack of integration and current skill set gaps. Therefore, it’s essential to think through both landscapes to figure out the right approach before simply jumping into an integrated model. The following considerations should be made by executives before adopting an integrated IT and OT model that has the ability to influence the organization’s strategy.

> “The OT technology at these shop floors tends to be old. This requires experience and time to be able to automate. On top of that, every plant seems to act differently with no unified database – it’s a struggle.”
>
> —Danielle Mazur

Critical considerations for OT in space

1. **Upgrade of current infrastructure to improve secure reliability at a lower cost.** Secure connection at air-gapped networks requires upgrading current infrastructure to edge computing and other technologies that can support the new demands. Data connectivity issues, multiple database formats, and inconsistent metadata make working with OT data challenging.

2. **Reduce siloed systems to have the ability to share data across IT and OT environments.** An ideal situation would be to harness data from the shop floor to help make data-driven decisions for deploying IT resources. The current challenge we see organizations face is the lack of infrastructure for aggregating data and database structures for meta-analysis. With separate roadmaps, strategies, and budgets for IT and OT organizations, the groups work in silos to overcome the challenges. Therefore, it is essential to integrate IT and OT into aligned strategy, governance, structure, and architecture.

3. **Solve the skill set gap and increase the team’s ability to respond quickly to service issues.** Traditionally, OT is managed by the shop floor team members who view it as an additional task to their job. With the increasing demands and requests from the IT team to patch and upgrade the current infrastructure, there is an expectation that OT team members will be able to fulfill those requests. What we are seeing, however, is that there is a skill set gap between how the OT team is operating today and how the IT teams expect the OT teams to perform. So what does this mean going forward? The IT and OT teams must collaborate and holistically integrate their skill sets. There is a need for skill set training from both sides to ensure implementation and maintenance success.

Why does this matter for OT cybersecurity more broadly?

Although the technology and cybersecurity landscape are changing with more visibility into OT challenges, it is still not considered a high enough priority. It lacks leadership buy-in (Lang, 2022b). Beyond the space industry leading the charge to integrate, other manufacturers need to build business cases and bring in subject matters to orchestrate practical conversations. On the IT side, it is essential to understand that although OT and IT seem similar, they have unique business cases and challenges. Treating these tools as the same is not recommended, and it even provides a disservice.

The following considerations can help organizations start thinking about mitigating risk in OT:

Strategy: Whether the goal is to reduce risk with OT by providing accountability to IT and OT teams or to drive successful integration of IT and OT, it is critical to build a top-down strategy that aligns OT with business objectives. Organizations need to carve out a budget for cybersecurity technology and staff to support IT/OT convergence to reduce risk.

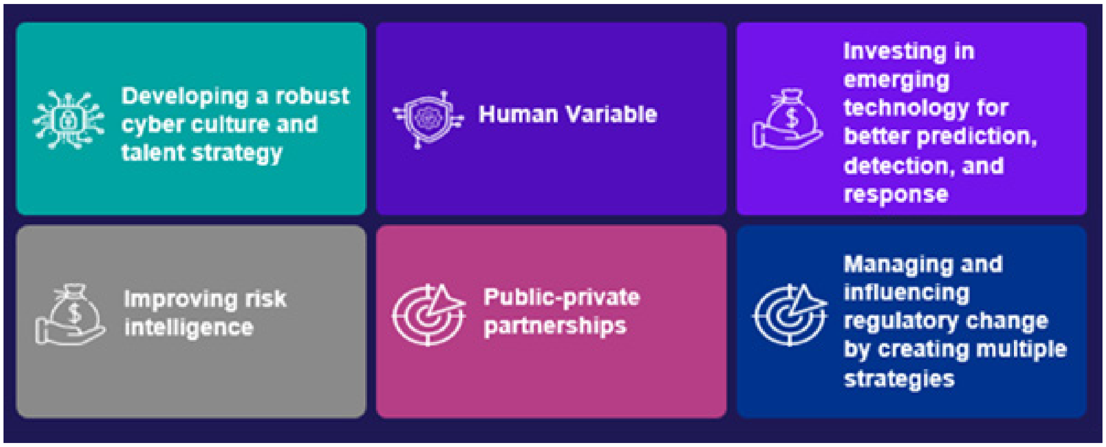
Technology: To succeed at scale, it is essential to set up a hosting and hardware infrastructure with a standard data stack for OT and IT. Even when data or systems might be plant driven, the infrastructure still needs a secure connection, especially when organizations shift to cloud. By creating a unified data structure, both OT and IT can pull expertise from each other and create a scalable strategy in the future.

Service delivery model: To make real-time decisions, it is critical to understand how organizations solve technology issues. OT procedures must be integrated and embedded within the IT processes (e.g., service desk tickets). This is critical because it allows a consolidated knowledge management view for solving OT and IT issues.

Organizational culture and skills: With any integration, change management becomes a necessity to ensure a smooth transition. Creating a team that is designed to be culture and change management champions could be a core driver as we shift to a modernized approach within IT/OT. The team would oversee culture, change, and resourcing needed throughout the process.

Governance: There are several ways to set up a governance structure in OT and IT. Three recommendations are (1) to create a project status meeting that forces these groups to share their tasks, (2) to have teams meet on a regular or structured cadence with dotted-line reporting to create an informal structure, and (3) to develop roles that consist of IT and OT experts with reporting structure shifting to a single executive (e.g., COO or CIO). The fourth option is a longer-term approach that we believe will have the greatest impact.

To learn more about how your organization can upgrade your OT strategy, cultivate a cybersecurity culture, or assess opportunities in the evolving space economy, contact KPMG for an in-person or virtual experience.



Developing a robust cyber culture and talent strategy

Human Variable

Investing in emerging technology for better prediction, detection, and response

Improving risk intelligence

Public-private partnerships

Managing and influencing regulatory change by creating multiple strategies

The Security Leader's Agenda offers a framework to address cybersecurity imperatives across the organization

References:

- Lang, J. (2022a). "Bridging the IT/OT Gap in Industrials and Manufacturing to Drive Digital Transformation," International Data Corporation.
- Lang, J. (2022b). "2022 Worldwide IT/OT Convergence Survey," International Data Corporation.
- Miske, B. (2023). "Experimentation by Design in the New Space Economy," LinkedIn.

Contact

Rik Parker
Principal
Cyber Security Services
KPMG LLP
rikparker@kpmg.com

Danielle Mazur
Manager
Ignition,
Cyber Security Lead
KPMG LLP
daniellemazur@kpmg.com

Lekshmy Sankar
Director
Advisory,
Cyber Security Services
KPMG LLP
lekshmysankar@kpmg.com

Lee Anderson
Manager
Ignition,
Chicago Innovation Lab Lead
KPMG LLP
leeanderson1@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.