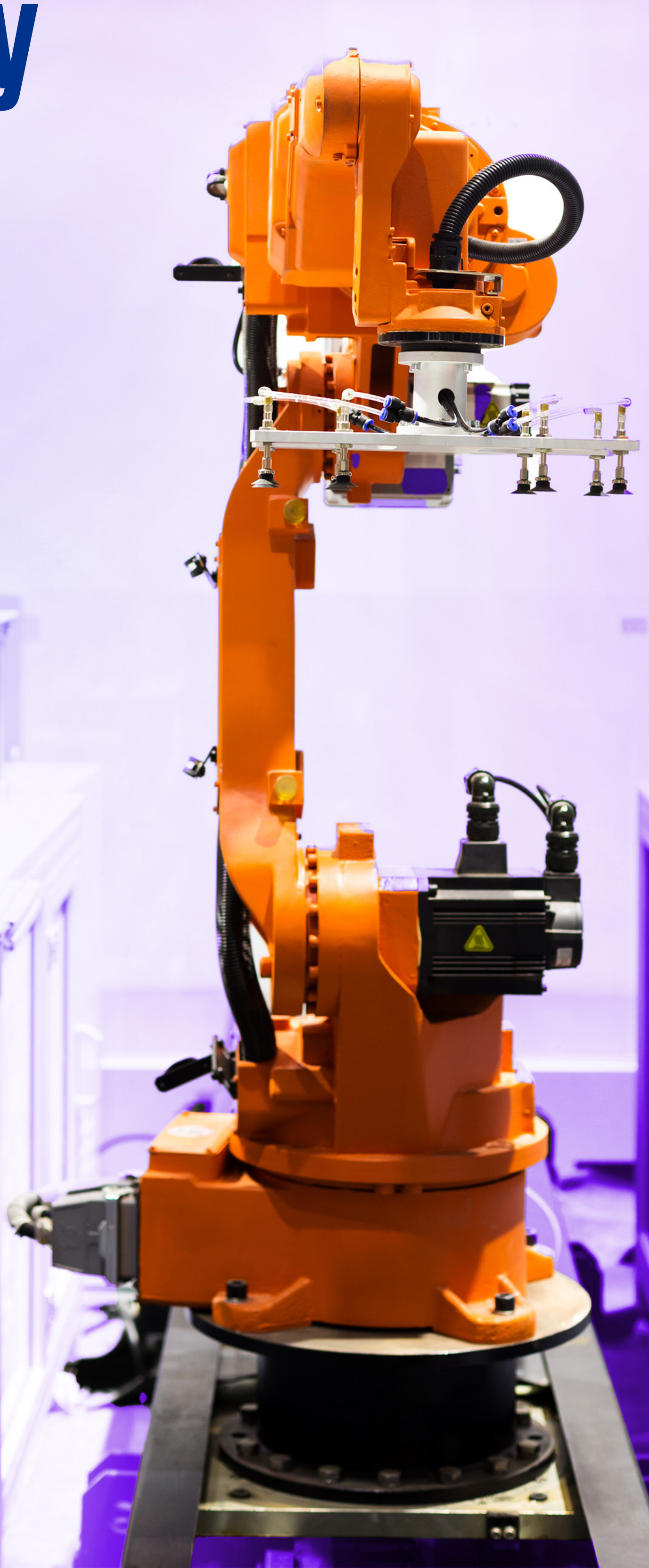
Cybersecurity in the space sector: It starts with the supply chain



January 2023

kpmg.com

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 to 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 series, analysis of cybersecurity considerations for the space sector, we first address the growing supply chain market—**Euroconsult measures the satellite manufacturing market at 29 billion U.S. dollars in 2022 up from 25 billion the previous year**[1]—and discuss why it is the foundation on which trust is built for this high-risk sector.

[1] EuroConsult, "Value of Space Economy reaches $424 billion in 2022 despite new unforeseen investment concerns," January 9, 2023

Cybersecurity in the space supply chain

Cybersecurity for the space sector starts before the assets are even built and then operational. Cybersecurity begins in the supply chain. A unique risk during manufacturing of connected devices is the physical development and handling of the equipment that will run the software, and store and transfer data. In the space sector, this is most commonly satellites but can also be launch vehicle components or Earth-based infrastructure. Before digital and electronic capabilities are operational and online, organizations must keep the hardware secure and uncompromised.

In a 2020 Gartner survey,[2] 71 percent of supply chain leaders surveyed cited cybersecurity as the most important capability for their workforce in the future. Across the space value chain, supply chains are the foundation that builds trust in a high-risk industry. Supply chain relationships are complex, involving dynamics from quality and pricing to timeliness and problem-solving capabilities. Trust in these attributes reflects on the customer and their stakeholder ecosystem, upstream and downstream.

This challenge speaks to what is unique about the space supply chain and the commonalities it shares with other hardware supply chains.

> “It is most effective to address cybersecurity in the earliest stages of building the components of the space architecture and embedding risk-reducing measures that meet the organizational mission and business objectives into the design and supply chain.[3]”

[2] Gartner, “Supply Chain Cybersecurity: 3 Future Advances,” 2022

[3] U.S. Department of Commerce, NIST, “Introduction to Cybersecurity for Commercial Satellite Operations (2nd Draft)” February 25, 2022

Key considerations for space sector supply chains:

1 Space assets are high-value targets. Supply chain risks for components that operate in remote environments and often store sensitive data or perform critical functions increase because infiltration can be planned early in the supply chain to decrease the likelihood of detection.

Further, many customers of space hardware are government and defense entities, increasing the value of the target to malicious actors. Finally, for many satellite companies, data is their product. When their primary resource is compromised, it can put the entire organization at risk.

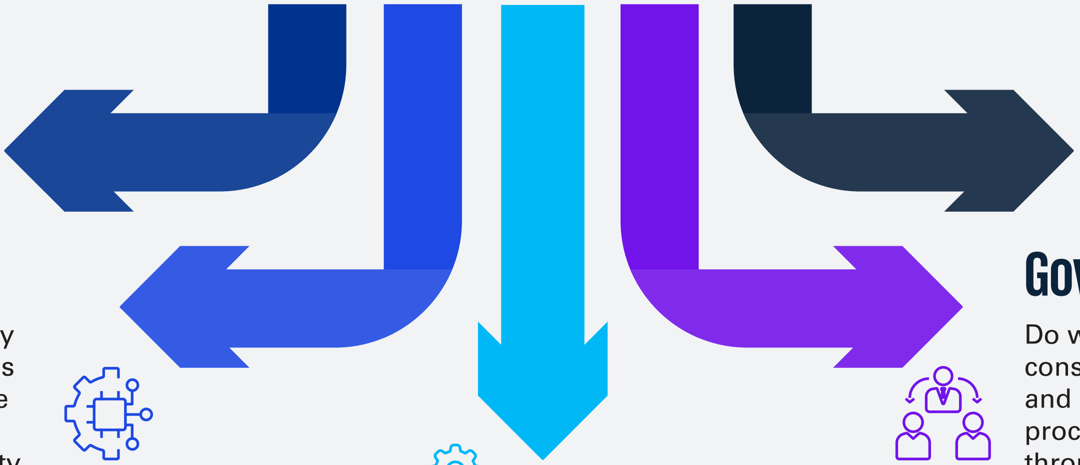
2 Due to the specialized nature of today's satellites, customization is widespread. The time up front can't be rushed to find the right long-term partners, anticipate lead times, and find the right pricing model for nonstandard orders. Hardware components are also very difficult, or impossible to repair once in space. Working with partners who understand the need to get it right during manufacturing is imperative.

3 Lead times can be extra-long not only because of raw materials and the international nature of the aerospace supply chain but also because of the rigorous testing required. While safety and resiliency tests are essential to the hardware components (e.g., radiation testing), space assets are also vessels for electronics and software that are highly vulnerable in their remote setting. Testing for ground control processes when a breach does occur can identify opportunities for automated response systems, personnel training, and firewall architecture.

Why does this matter for supply chain cybersecurity more broadly?

Though there are unique characteristics to the space supply chain, there are also commonalities with other sectors. Connected devices, from smartphones to smart refrigerators and smart cars, are commonplace today. Learnings and standard practices can be shared across sectors to anticipate breach attempts and minimize damage when breaches occur. Improvements can also be made to the existing controls discussed above, including finding the right suppliers and partners, establishing a chain of custody for parts, governance, and rigorous testing.

The following considerations can help organizations start thinking about mitigating risk in the space supply chain:



Strategy

Do our strategy and projections account for the time and cost of cybersecurity mitigation in our upstream operations?

Technology

Are we proactively managing moments of vulnerability, such as technology and equipment upgrades and system updates?

Service Delivery Model

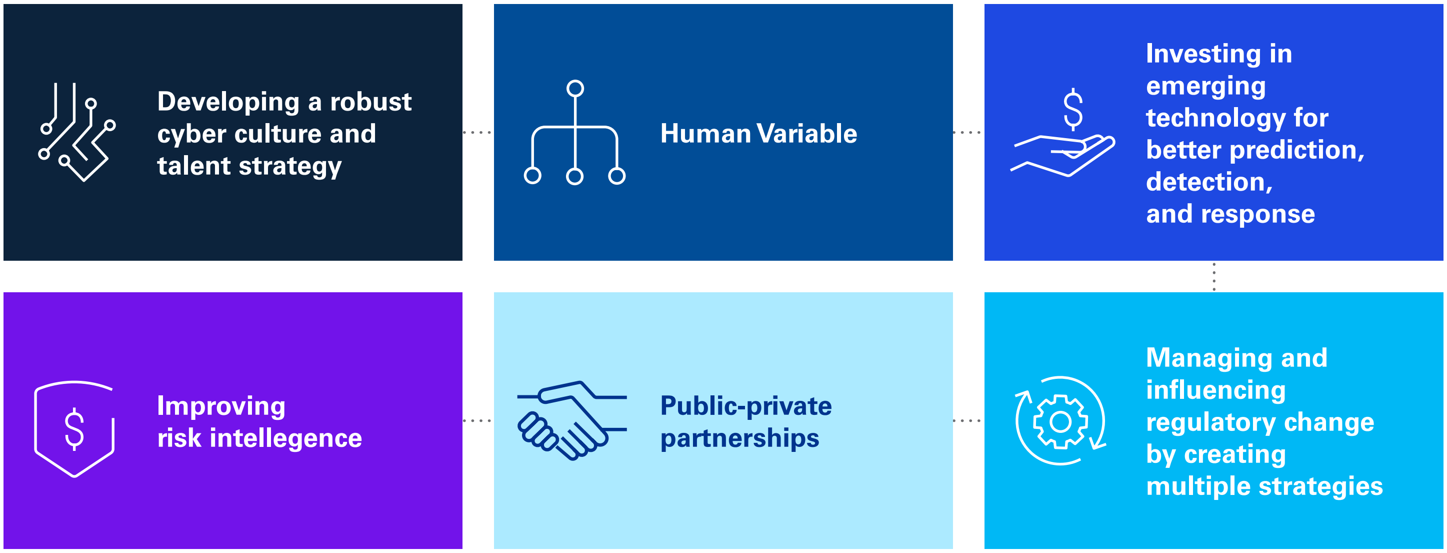
Are we properly communicating the precautions and procedures we have in place to our customers to instill trust and know their role in preventing incidents?

Organizational Culture and Skills

Are our supplier and a third-party workforce equipped to recognize a breach attempt and trained to act to protect the organization's information?

Governance

Do we have consistent and adequate procedures throughout our supplier network to identify cybersecurity risks when they arise?



Developing a robust cyber culture and talent strategy

Human Variable

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

Improving risk intellegence

Public-private partnerships

Managing and influencing regulatory change by creating multiple strategies

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

Additional reading

(1) Wilson Center, "From Supply Chains to Spacecraft: Taking an Integrated Approach to Cybersecurity in Space," September 16, 2021

(2) Via Satellite, "Key Considerations for Satellite Cybersecurity in 2023," January 31, 2023

(3) World Economic Forum, "Will the battle for space happen on the ground?" May 25, 2022

(4) Space News, "Satellite supply chains coming under increasing scrutiny," March 22, 2022

To learn more about how your organization can manage supply chain risk, cultivate a cybersecurity culture, or assess opportunities in the evolving space economy, contact KPMG Ignition for an in-person or virtual experience.

Contact us

Rik Parker
Principal,
Cyber Security Services
E: rikparker@kpmg.com

Danielle Mazur
Manager,
Ignition Cyber Lead
E: daniellemazur@kpmg.com

Lekshmy Sankar
Director,
Cyber Security Services
E: lekshmysankar@kpmg.com

Lee Anderson
Manager,
Chicago Innovation Lab Lead
E: 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 based on authorities that are subject to change. Applicability of the information to specific situations should be determined through consultation with your tax adviser.