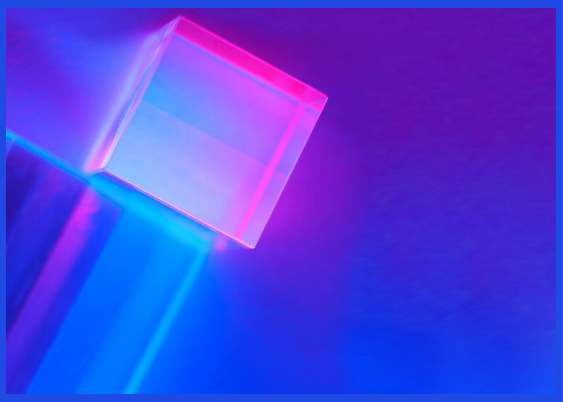
Cybersecurity in the space sector



Culture driving successful security programs

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 the cultural implications for maintaining both a secure sector and a secure organization.

Culture in the space sector

As the space sector undergoes rapid change and the usage of space assets grows, securing legacy and emerging satellite missions and the manufacturing of satellites and rockets becomes vital. The increased level of investments in the space sector is opening the doors to new opportunities and triggering the threat environment to shift. With an increased focus on innovation and rapid-prototyping, cybersecurity risks should be a priority given the criticality of space infrastructure to our everyday lives and to essential services such as military, utilities, transportation, and emergency communications. In 2022, it was brought to light that cyberattacks on satellites servicing one country could disrupt critical national infrastructure in another (World Economic Forum). The space industry relies on the ability to create a cyber-safe and resilient space industry.

As the infrastructures become more complex, the industry is evolving into full end-to-end services that involve many stakeholders operating different parts of the infrastructure. The risks of cybersecurity must be elevated across the entire value chain (e.g., supply chain, operations, operational technology, third-party relationships, etc.). "Some of the most impactful changes needed aren't linked to digital solutions, but instead focused on the human element—realigning the mindset and daily behaviors of employees to adopt activities that prioritize good security habits" (Breah Sandoval, KPMG LLP director). In this article, we focus on the culture considerations in the space sector. We explore culture from two different angles: (1) cybersecurity culture within the space industry as a whole and (2) the cybersecurity culture within each company.

Starting with cybersecurity culture within the space industry

Cyber threats to commercial satellites are no longer hypothetical as we are seeing an increase in economic tensions from Russia and China. The increased threats paired with the rapidly evolving technology that integrates unique environments with dependencies of critical infrastructure and societal resilience has caused the sector and government to consider new approaches, tactics, and policies. It is clear that no one organization alone can fully manage cyber threats to the space sector to ensure global security.

With the high volume of regulatory and compliance requirements and cyber threats in the space sector, more and more we are seeing the culture evolve in the space sector to be collaborative across companies and government agencies. The collaborative culture allows companies to have more insight into best-in-class tactics to ensure their infrastructure, operations, and space systems are secure and threat informed, and that the organizations are compliant with regulatory and compliance requirements.

Today we are seeing the U.S. government developing clear policies to manage the cyber threat space, the Department of Defense creating clear standards for its acquisition programs, and industry and government leaders pushing for a culture change across the space community to integrate cybersecurity more effectively into every organization.[1] To better understand how this culture is evolving, we will look at **Aerospace Corporation** to understand frameworks developed for operating securely, **Consultative Committee for Space Data** (CCSDS) to understand how regulatory and compliance frameworks are evolving to keep up with the changing requirements, and **Space Information and Sharing Analysis Center** (Space ISAC) to understand what is being built to allow for clear lines of communication to support information sharing prior to, during, and after a cyber incident.

1. The Aerospace Corporation developed SPARTA to help developers and network defenders alike to understand the types of space-cyber tactics, techniques, and procedures they need to be resilient against. SPARTA serves to ensure the space-cyber community is empowered to continually educate engineers and system defenders so they can overcome the unique cyber-threats they face in the domain. Aerospace's goal is to document these TTPs so that space developers understand how threat actors could attempt to attack their space infrastructures and systems (Aerospace.org).
2. "The Consultative Committee for Space Data Systems (CCSDS) is a multinational forum for the development of communications and data systems standards for spaceflight. Leading space communications experts from 28 nations collaborate in developing the most well-engineered space communications and data handling standards in the world. The goal is to enhance governmental and commercial interoperability and cross-support, while also reducing risk, development time, and project costs." Countries are working alongside one another to develop minimum cyber measures to help satellite companies ensure their operations address specific vulnerabilities and abide by standards related to the space industry (CCSDS).
3. "The Space ISAC serves to facilitate collaboration across the global space industry to enhance our ability to prepare for and respond to vulnerabilities, incidents, and threats; to disseminate timely and actionable information among member entities; and to serve as the primary communications channel for the sector with respect to this information." (Space ISAC)

The culture of collaboration between governments, satellite manufacturers, operators, software developers, and service users in the space sector itself is one element of culture that it critical to secure the infrastructure. Each has a role to play, including the sharing of lessons and experiences from each domain. As space systems become ever more closely integrated and the distinctions blurred, a collaborative and informed exchange is needed between what has traditionally been seen as separate areas of cyber threat management. (World Economic Forum)

Cybersecurity within the organization

Continuing off the discussion around the ever-evolving and complexity of the space infrastructure, the other cultural element critical for securing space systems is the culture within each organization. Having a risk-resilient culture across each player and across the entire value chain is critical to ensure that the responsibility and reliability for the ultimate security and resilience of the services is supplied. As organizations build their security strategy, best practices, and frameworks, the strategy needs to highlight cyber culture. Often the word "culture" is left out when discussing a security strategy for companies. Without a healthy and risk-forward security culture in place, strategies tend to fall apart.

"Culture eats strategy for breakfast."—Peter Drucker, "Management Thinking" strategist

Within organizations, we are seeing the following cultural gaps: (1) burnout of CISOs and employees, (2) very few dedicated resources to secure their entire space value chain; and (3) lack of cyber culture awareness training.

[1] Via Satellite – Key Consideratoins for Satellite Cybersecurity in 2023; January 6, 2023

A strong cyber culture starts at the top and requires an investment in both people and systems. With a lower-than-average tenure (approximately 1.9 years), security leaders struggle to keep momentum, gain traction, and see long-term strategies through completion (Information Systems Security Association). Security leaders and their teams are running from crisis to crisis. With a growing need to address near-term priorities, security leaders are under tremendous pressure to respond and have little time to be proactive. Lack of proactive activity leads to stress and unhappiness in their role and in their team. The psychological impact of being in this state directly affects decision-making and performance of leaders and their team.

Lack of proactivity in the space sector can be detrimental to the security of value chain. Additionally, constant shifts in leadership and the transitioning of roles can potentially lead to missed security protocols and a lag in ensuring the organization is staying up to date with standards.

Though on the rise, the maturity of security teams within space organizations is still relatively immature. There is a -3.43 million gap in the cybersecurity workforce. In 2022 alone, the demand for cybersecurity professionals was around 8.09 million while the global cybersecurity workforce was 4.66 million people. Companies need to continue to strategize on how to best approach their security programs based on the current workforce gap. A great use case to follow for maturing the security function is NASA's Cybersecurity and Privacy Governance (CSPD) function whose objective is to develop and manage policies, procedures, and programs to ensure effective governance, risk management, and compliance activities that maximize the value of the agency's cybersecurity program.

With all the cybersecurity requirements and frameworks out there for securing the space industry, many companies think they are taking care of the obvious vulnerabilities. One area that is missed quite frequently is the risk training of the organization's employees. If there is not the right user awareness and risk-oriented training in place, then one click from one bad vendor could result in a huge cyberattack. Security teams need to ensure their training.

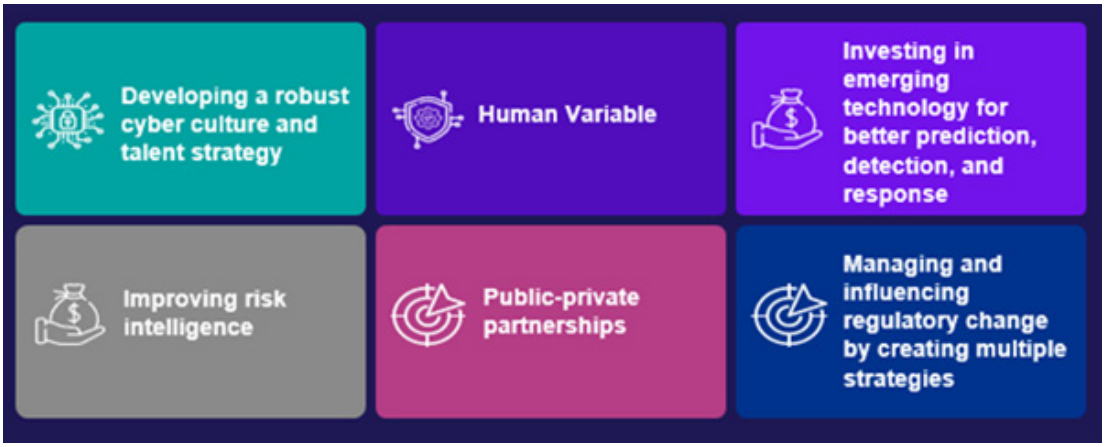
Why does this matter for operational technology cybersecurity more broadly?

The cybersecurity culture within organizations is continuing to evolve, but it is not quite hitting the mark at most companies. "An organization can implement state-of-the-art DevSecOps solution and premier safety policies and procedures and still fail to achieve desired results due to the persistence of outdated ways of working among employees. To affect changes to cultural norms, we must focus on identifying and promoting specific desired behaviors that support good cybersecurity hygiene, while also identifying common behaviors that present risk. Security teams need to identify core values within the corporate culture that motivate your employees' behavior and steer their daily ways of working." (Breah Sandoval, KPMG LLP director)

The following considerations can help organizations start thinking about culture within their organization:

1. Executive leadership support and buy-in
2. Culture framework fit for purpose
3. Communication of cyber training and awareness across the entire organization
4. Consistent engagement and positive reinforcement.

To learn more about how your organization can cultivate a cybersecurity culture, contact KPMG for an in-person or virtual experience.



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

References:

1. World Economic Forum, "Will the battle for space happen on the ground?," May 2022.
2. Aerospace.org., "Understanding space – cyber threats with the sparta matrix." October 2022.
3. Space ISAC and Information Sharing and Analysis Center, January 2023.
4. Consultative Committee for Space Data Systems, January 2023.
5. National Aeronautics and Space Administration, October 2022.
6. Information Systems Security Association, Nominet, Forbes, and Korn Ferry.

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