Defending the aerospace and defense sector

Closing gaps in A&D cybersecurity

kpmg.com

Your organization is under constant and malicious attack. Your defenses are under siege. Your assets are under threat. And your people are being unknowingly subverted. Are you confident in your cybersecurity?

Right across the aerospace and defense (A&D) sectors, the cyber threat is rising. Hackers, hacktivists, organized crime syndicates, state-sponsored actors, and even bored teenagers are constantly testing cyber defenses. And when they find a breach, they waste no time sowing havoc.

Thankfully, cybersecurity and defense capabilities remain high across the sector and (for the most part) the major players and their suppliers have avoided any massive intrusions. Capabilities are so strong, in fact, that a growing number of defense players now offer cybersecurity "as a service" to other industries and business sectors.

But that does not mean that the sector is immune to the growing cyber threat. In fact, our experience suggests that A&D organizations may continue to face significant exposure that could put their organizations' futures at risk. Many may not even be aware of the extent of the threat.

We believe that A&D organizations must redouble their cybersecurity efforts by working across the enterprise, the value chain and the ecosystem to close any remaining gaps. And we believe there is no time to waste. ■

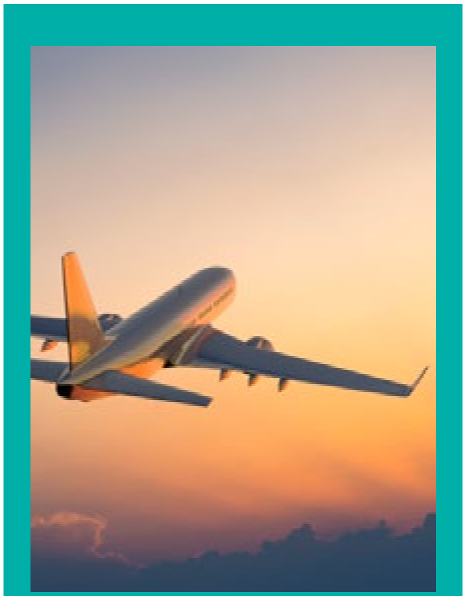
A fortress erected

When it comes to cybersecurity, the aerospace and defense (A&D) sectors have every reason to be confident. The reality is that the sector has not yet suffered any "major" cyber breaches (that we are aware of). No aircraft have fallen out of the sky due to a denial of service attack or electronic hijacking (again, that we are aware of). Hackers have yet to wrest control of an active military vehicle by electronic means alone.

In part, this high level of cyber awareness and security is driven by regulation. Commercial aerospace and defense organizations have always been a priority target for attackers, particularly terrorist and state-sponsored espionage groups. Ever since the first hijacking of a commercial aircraft, security—physical and cyber—has been top of mind for the FAA, the DoD, and other related regulators.

Not willing to take any chances, the two sectors have also taken unprecedented measures to help ensure their cyber defenses, particularly at the product level. Commercial aerospace manufacturers, for example, have completely segregated their operational flight systems from their (ever-growing) entertainment systems. To date, this has effectively eliminated the risk of a passenger taking down the aircraft through direct hacking.

In the defense sector, products tend to be secured through the use of "closed systems" that (theoretically at least) are segregated from the rest of the network. At the same time, state secrets, design plans, financials, and other valuable data "jewels" have been locked up in ever-tighter rings of security. Defense players have become so adept at cybersecurity (either through development or acquisition) that many now offer their services to other industries, creating an important new growth opportunity for the sector. ■



"Commercial aerospace manufacturers, for example, have completely segregated their operational flight systems from their (ever-growing) entertainment systems"

Tracking abnormal threat vectors

While all business sectors—particularly financial services, healthcare, and retail—face a growing cyber threat, the A&D sector has become the target of particularly sophisticated and ruthless actors.

On the defense side, not only must manufacturers contend with the usual threat of IP theft by organized crime rings, they are also increasingly facing off against very well-resourced state-sponsored actors. Design schematics are often the top prize. But these spies are also snapping up data from across the organization—from employee records to maintenance reports.

The commercial aerospace sector faces very similar threat actors, but also some unique challenges. Very few other industries, for example, need to worry about suicidal customers bent on massive destruction. But ever since 9/11, commercial aerospace manufacturers have been acutely aware of the threat from inside the plane as well as from outside.

It is not just the threat actors that are more dangerous for the A&D sectors, it is also the risks. The bottom line is that military hardware and commercial aircraft both hold a high level of lethality. And this means that A&D manufacturers are held to a higher standard. An intrusion into a retail bank ATM is one thing. Bringing down an airplane or turning a military drone on a civilian population is another thing entirely.

Besides the high potential for loss of life, the most immediate and obvious risks for the A&D sector are reputational and financial. The loss (or loss of control) of a multimillion-dollar product due to cyber attack would have an immediate impact on the manufacturer's reputation and that, in turn, would have a significant financial impact in this highly competitive environment. Order books could quickly dry up, and access to military contracts could be lost.

Even the loss of "lower-grade" data could create reputational and financial challenges. A breach into employee data, for example, can attract a significant regulatory fine and penalties if defenses were not deemed up to standard. The loss of financial data may have an impact on stock prices and valuations. Losing design schematics and research outcomes to a less ethical competitor could have long-term financial implications. ■

> *"The bottom line is that military hardware and commercial aircraft both hold a high level of lethality".*

Closing the gaps

The challenge for today's A&D sector is two-fold. On the one hand, the sector must strive to remain not just one but two steps ahead of the cyber threat. They must continue to invest into new capabilities, technologies, and ideas. They must remain vigilant against a highly adaptive threat. And they must place more focus on embedding security into their products from the design phase.

At the same time, however, A&D players will need to ensure they are closing any gaps in their current cybersecurity stance. Our experience suggests there are a number of areas that may require urgent attention.

One area of immediate concern, particularly for the defense sector, is the heightened risk of cyber attack through third parties. Indeed, as the A&D sectors' supply base widens to incorporate new technology players, service providers, and infrastructure, many manufacturers are losing sight of the risks that these relationships create. At the same time, new regulations (such as NIST SP 800-171) are sharpening the urgency for manufacturers and the supply base.

Access control is also an ongoing challenge for many A&D organizations. Most are fairly good at onboarding their new employees and granting access when job roles and requirements change. But few are as good at closing down employee access once an individual leaves the organization or changes roles. The loss of what might be regarded as a low-level access code could have unexpected implications.

The commercial aerospace sector (and, to a lesser degree, defense players with products or services in nondefense industries) must also start to focus on a new and growing gap: the protection of consumer data. Intentional or not, airplanes capture masses of consumer data – from wi-fi connections, entertainment selection and even USB drives plugged into the system – and few commercial aircraft OEMs have yet to create a robust strategy for protecting this growing source of data. ■

"Most are fairly good at onboarding their new employees and granting access when job roles and requirements change.

But few are as good at closing down employee access once an individual leaves the organization or changes roles."

Staying two steps ahead

We believe that the path to the long-term security of the A&D sector lies in heightened standards, improved data governance, and deep industry cooperation.

At an industry level, standards will largely be driven by industry and regulatory pressure. Efforts are already underway to develop a Service Organization Control (SOC)-type attestation program to assess the security controls and processes within third-party suppliers in the sector. Greater focus must be placed on driving improved internal standards as well, particularly related to access control and consumer data.

Improved data governance will also be key. A&D executives will need to focus on ensuring that policies, controls, and training reinforce the need for heightened risk awareness and data protection across the business. Most organizations could also improve the way data is currently categorized, stored, and transferred between systems and suppliers.

Most importantly, however, the industry must continue to work together to share best practices, threat awareness, incident reports, and other critical information in a way that improves the overall security and resilience of the sector. This will certainly require collaboration with new partners in the value chain and may necessitate the development of consortiums or joint ventures.

Cybersecurity is a critical capability for players in the A&D sectors. But while the industry has fared well so far, there is a constant danger of complacency. We believe it is time for A&D organizations to redouble their efforts. There is no time to waste. ■

Contacts

Doug Gates
Global Sector Chair, Industrial Manufacturing
T: 404-222-3609
E: dkgates@kpmg.com

Tom Mayor
National Service Group Leader,
Industrial Manufacturing Strategy
KPMG US
T: 216-875-8061
E: tmayor@kpmg.com

Ronald Plesco
Principal, Cyber Investigations Lead
KPMG US
T: 717-260-4602
E: rplesco@kpmg.com

Frederick Rica
Principal, A&D Sector Cyber Leader
KPMG US
T: 973-912-4524
E: frica@kpmg.com

kpmg.com/socialmedia