AEROSPACE & DEFENSE

Cyber resilience as a necessary component for aerospace and defense digital transformation

Technological changes come fast and furious, and many aerospace and defense manufacturers are embracing this continuous technological evolution to help them stay competitive. This digital transformation helps position manufacturers to better achieve broad goals, like increased revenue and improved profitability, as well as more focused goals, such as new product development and the introduction of service-based business models.

Manufacturers that commit to digital transformation gain access to advanced manufacturing processes that help them deliver cost-effective products and services. These advanced technologies also allow manufacturers to make existing products smarter by using sensors and connectivity, which can also unlock a torrent of rich, new, valuable data.

Alongside the benefits of technological advances, however, come some inherent challenges—of which **cybersecurity risks can be some of the most problematic** and potentially damaging.[1] In an era of digitization where cyberthreats continue to rise, aerospace and defense manufacturers must ensure they're using their digital transformation to also help them become a more cyber-resilient business.

A **cyber-resilient** business brings together the capabilities of cybersecurity, business continuity, and enterprise resilience, in order to introduce innovative offerings and business models securely, strengthen customer trust, and grow with confidence.[2] Cyber resilience is a critical business imperative that accompanies an effective growth strategy. With the multiple rules and regulations required to achieve and maintain an approved-supplier status to the Department of Defense (DoD), defense contractors especially need a cyber resilience strategy to stay in business and achieve their digital transformation goals.

Make cyber resilience a business mandate

Nearly all aerospace and defense manufacturers face the very real threat of losing business without a cyber resilience strategy. Strict governmental regulations mandate that suppliers must follow and prove they maintain a culture of cyber resilience. If a manufacturer can't prove compliance with these regulations, it loses eligibility to bid on and secure lucrative government contracts.

For instance, one of the regulations that affects aerospace and defense manufacturers is the Defense Federal Acquisition Regulations Supplement (**DFARS**) set of rules.[3] These rules include a mandatory clause based on the National Institute of Standards and Technology (NIST) publication, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations—which states that DoD contractors that process, store, or transmit Controlled Unclassified Information (CUI) **must meet the DFARS minimum security standards**.[4]

According to an Accenture survey of aerospace and defense executives:

- 75% believe cybersecurity risks will grow substantially in the next few years as they adopt new and enhanced business technologies[8]
- 69% say they expect data exchanges with strategic partners and other third parties to increase cyber risk[9]
- 89% anticipate that the number of third parties and strategic partners in their ecosystems will increase in the next three years[10]

All defense suppliers were mandated to be DFARS compliant by the end of 2017. However, the supplier community held **the perception that the DoD would be hesitant** to cut non-compliant suppliers due to an already low number of suppliers available to meet the growing demand for products and materials.[5] As a result, many contractors were not compliant by the deadline, and many are still not DFARS compliant today.[6]

That is in the process of changing right now. On January 21, 2019, the Undersecretary of Defense issued a memorandum instructing the director of the Defense Contract Management Agency (DCMA) **to begin auditing contractor compliance** with the DFARS clause.[7] Defense suppliers that haven't prioritized achieving DFARS compliance will now need an aggressive plan to meet and maintain compliance.

These plans need to include a comprehensive review and action plan to improve the cyber resilience of software systems, both inside manufacturing operations and out in the supply chain.

Fortify the software foundation

Aerospace and defense manufacturers have been repairing and patching their ERP systems to meet minimum security and regulatory requirements throughout the years. However, it will soon become difficult to maintain business operations with just a repair-and-patch strategy. The tools used to keep legacy ERP systems updated will no longer be sophisticated enough to combat cyber threats coming now and in the future.

Many of these tools are outdated because computers and related equipment have an average lifetime of around nine years before manufacturers typically choose to replace or decommission them. Heavy machinery lasts even longer—from 26 to 34 years, on average. Manufacturers are also more likely than other industries to use a software infrastructure based on Windows® XP or Windows XP 64-bit, which have been **unsupported** since 2014.[11]

In order to achieve cyber resilience, aerospace and defense manufacturers need to prioritize the upgrade of their software infrastructures—which include mission-critical ERP systems that connect with various software systems across and outside their organizations.

Embracing innovative technologies, like cloud-based computing, is paramount for successful cyber resilience. While it may seem counterintuitive, moving mission-critical computing infrastructure to a cloud-based environment is important for achieving the highest levels of cybersecurity. According to Gartner, public cloud infrastructure as a service (IaaS) workloads will see **at least 60% fewer security incidents** than those in traditional data centers.[12]

5 questions to start building your cyber resilience strategy

Not sure where to start improving your business to be cyber resilient? Start by thinking like the attackers who would want to compromise your systems. Here are five questions to get you started:

1. What software assets do we have?
2. Where is our most important information stored?
3. What software systems would cripple our business if compromised?
4. How is our software connected to other partners and suppliers?
5. How old are our software systems?

Extend cyber resilience into the supply chain

Aerospace and defense manufacturers' value chains and supply chains are linked electronically and across geographies. **Supply chain attacks ballooned by 78% in 2018**, with attackers initiating supply chain threats through software updates and other entry points, spreading security threats both inside an organization and across the supply chain to the connected organizations.[13]

Aerospace and defense manufacturers need to initiate a cyber resilience infusion across operations, starting within their own enterprises. Executing this mission first requires a clear picture as to what software-based assets the manufacturer has, and what threat each of these assets may pose to its business.

A comprehensive audit may prove overwhelming, with manufacturers not knowing where to begin. Manufacturers should **review software assets that support essential business functions**, including technology that aggregates data, stores intellectual property, and isn't understood by the user—particularly older technology embedded within the hardware.[14]

Embrace cyber resilience as a foundation for growth

DFARS compliance is aerospace and defense manufacturers' biggest incentive to prioritize cyber resilience. Beyond just meeting federal regulation requirements, manufacturers will find that embracing a cyber-resilient strategy now will provide a foundation for business growth and establish an environment for successful digital transformation.

Aerospace and defense manufacturers who commit to a strategy and culture of cyber resilience will become stronger competitors. With pervasive cyber resilience, they can grow their businesses with the knowledge that cyberattacks will have minimal impact on their daily operations and reputation. In addition, they'll have comprehensive processes and software systems in place to safely integrate suppliers and partners into their supply chains—achieving comprehensive and secure digital transformation.

1 Robin Lineberger, Aijaz Hussain, Tim Hanley, Vincent Rutgers, and Brenna Sniderman, "Aerospace & Defense 4.0: Capturing the value of Industry 4.0 technologies," Deloitte; February 12, 2019.
2 Accenture, Gaining ground on the cyber attacker: 2018 The State of Cyber Resilience, April 10, 2018, p. 5.
3 "DFARS Cybersecurity Requirements," National Institute of Standards and Technology, April 26, 2019.
4 "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," National Institute of Standards and Technology, June 7, 2018.
5 National Defense Industrial Association, Implementing Cybersecurity in DoD Supply Chains, July 2018, p. 2.
6 Ibid.
7 Department of Defense, Memorandum for Commander, U.S. Cyber Command: Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review, January 21, 2019.
8 **Accenture, Securing the Digital Sky**: Cyber Resilience in Aerospace and Defense, July 17, 2019, p. 3.
9 Ibid., p. 5.
10 Ibid., p. 5.
11 Trend Micro, Securing Smart Factories: Threats to Manufacturing Environments in the Era of Industry 4.0, April 3, 2019, p. 9.
12 Kasey Panetta, "Is the Cloud Secure?," Gartner, March 27, 2018.
13 Symantec, 2019 Internet Security Threat Report, 2019, p. 1.
14 Deborah Abrams Kaplan, "As supply chains get tech savvy, is cybersecurity keeping pace?," Supply Chain Dive, April 16, 2019.

Learn more ›

infor

Gold
Channel Partner

Follow us:

GODLAN

INF-2338855-en-US-0620-1

Godlan, Inc.
15399 Canal Road
Clinton Township, MI 48038
586-464-4400
info@godlan.com
www.Godlan.com