AEROSPACE CYBERSECURITY:

ENDURING **CHALLENGES**
ENDURING **SOLUTIONS**

BRINGING CYBER PROTECTION TO THE HEART OF THE AEROSPACE INDUSTRY

This white paper explores findings and insights from the 2020 American Institute of Aeronautics and Astronautics (AIAA) Aerospace Cybersecurity Market Study, as well as the AIAA aerospace community's program for addressing its members' and the aerospace industry's cybersecurity needs.

AIAA
SHAPING THE FUTURE OF AEROSPACE

Making the Case for Enhanced Cyber Protection

Growing satellite constellations are a case in point for enhanced aerospace cybersecurity. Without robust cybersecurity protocols, hackers could take control, shut them down, deny user access, or jam their signals. Such disruptions could cause major harm to space operations and to critical infrastructure dependent on these satellites, such as electric grids, water systems, and transportation networks.

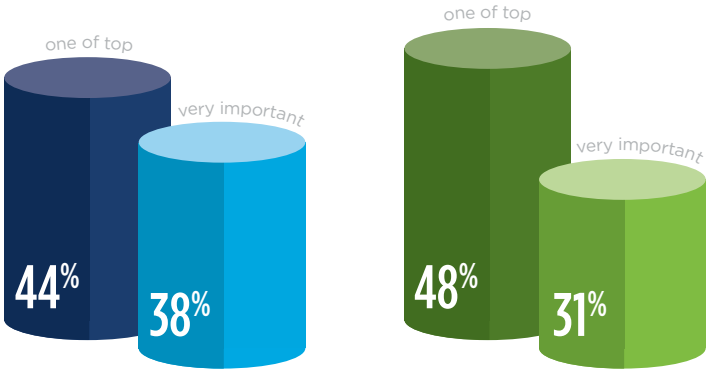
Historically, aerospace has been hesitant to embrace mainstream cybersecurity. The subject has not been emphasized in most undergraduate aerospace curricula nor consistently included in aerospace development and manufacturing processes. Rather, we have seen only small bursts of focus in both areas. We must move toward a more routinized approach from education, through concept development, design, manufacturing, and on to operations. This is a big task requiring engagement throughout the aerospace community and supply chain.

There are two real-world factors causing our industry to take a more serious approach to cybersecurity. The fear of an attack or breach of an aerospace company's systems that results in operational disruption or the exposure of proprietary information always looms. We have seen numerous examples of disruptive ransomware and cyber espionage across the spectrum of aerospace enterprises – manufacturers, airlines, and government agencies have all been victims of cyber attacks, resulting in the loss of proprietary data and the interruption of operations.

Then there is the more subtle challenge – the emergence of new cybersecurity requirements on the aerospace industry. When cybersecurity regulations hit the power grid and commercial nuclear industries over the past decade, the effort of complying and staying in business under the new guidelines was costly and complex. These companies endured significant organizational stress adapting their people, processes, and technologies to the new regulations. Many incurred unexpected capital and consulting costs to satisfy new cybersecurity audit requirements. The aerospace industry is primed for similar challenges:

- The DoD's Cybersecurity Maturity Model Certification (CMMC) requires every company that does business with the federal government to comply with a certain level of enterprise-level cybersecurity requirements, based on work provided.
- Space Policy Directive 5 (SPD-5) requires cybersecurity principles and practices currently applied to terrestrial systems be applied to space systems and integrated into every phase of the space system life cycle.
- An October 2020 U.S. Government Accountability Office report recommended more rigorous and extensive focus on cybersecurity in Federal Aviation Administration aircraft inspections and tests.

Cybersecurity is considered important and has become an urgent "top" priority to just under half of aerospace professionals.



"Cybersecurity is an issue of growing prominence within the aerospace community … as we continue to drive this dynamic progress forward, we must aggressively protect aerospace with strong cybersecurity practices."

DAN DUMBACHER, Executive Director, American Institute of Aeronautics and Astronautics

American Institute of Aeronautics and Astronautics
12700 Sunrise Valley Drive, Suite 200, Reston, VA 20191-5807 I 703.264.7500 I aiaa.org

AIAA is Committed to Growing Cybersecurity Awareness

AIAA spent 2020 bringing cybersecurity front and center by hosting events, technical talks and presentations, and educational opportunities around the topic. Importantly, AIAA commissioned a Cybersecurity Market Study to guide its efforts (detailed results discussed below). These efforts are the beginning of the long-term commitment from AIAA on this topic.

The AIAA members who comprise the Aerospace Cybersecurity Steering Committee have been the driving force behind AIAA's increased focus on this topic. The group includes senior AIAA members and outside experts who collectively engage and advise the Institute on what it should/should not be doing in terms of cybersecurity. Going forward in 2021, they are empowered with the resources and guidance they need to make real progress.

At the grassroots level, AIAA members interested in aerospace cybersecurity formed their own Aerospace Cybersecurity Working Group. This working group has spearheaded delivery of technical papers to AIAA forums, and it also plays a critical role in the creation of AIAA's upcoming aerospace cybersecurity learning offerings.

AIAA has entered into a cooperation agreement with the Aviation Information Sharing and Analysis Center (ISAC) and will soon conclude such an agreement with Space ISAC, which already has collaborated with AIAA during the recent ASCEND event. These partnerships between AIAA and the ISACs, in their frontline roles in the cyber defense of aerospace, foster open dialogue and cooperation around this topic. These relationships provide for collaboration on learning activities to better prepare the aerospace and aviation cybersecurity workforce. Publications and forum content will serve to raise awareness of cyber risks, including best practices and lessons learned; threat actors; tactics, techniques, and procedures (TTPs); and more.

The AIAA Space Policy Podcast dedicated its May 2020 episode to cybersecurity, hosting Matthew Scholl of the National Institute of Standards and Technology (NIST), who shared compelling insights on advancing cybersecurity in space.

Everyone in our industry is energized by our growing space economy and promising new aviation innovations. AIAA believes we must protect that momentum and act now.

Aerospace Cybersecurity: What the Community Thinks

AIAA's focus on cybersecurity is driven by our members and the aerospace community. In 2020, AIAA commissioned an Aerospace Cybersecurity Market Study that measured the aerospace community's and AIAA members' level of concern with cybersecurity. Nearly 75 percent of the members who participated expressed strong interest in the steps AIAA is pursuing to promote cybersecurity awareness. Findings from the study include the following.

Cybersecurity Expertise Already Embedded in Several Areas

Key areas of need for cybersecurity expertise and solutions include application security, disaster recovery plans, and oversight in the supply chain.

› Information, network, and operational security are the areas about which the industry feels most confident and is likely to have solutions in place. AIAA members are somewhat better positioned than others in the industry in terms of having a cybersecurity solution in place for:

- Information security
  (82% members, 74% industry professionals)
- Network security
  (81% members, 70% industry professionals)
- Operational security
  (81% members, 75% industry professionals)

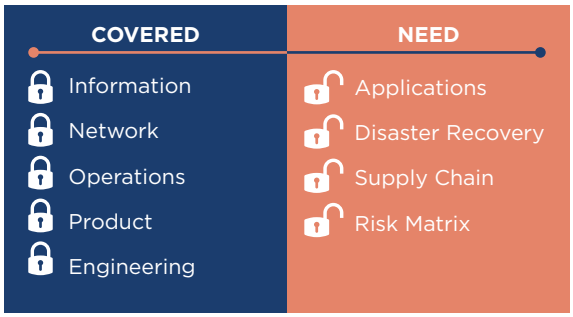
› The survey identified application security and disaster recovery as the areas of greatest need for tailored aerospace cybersecurity solutions. Again, AIAA members are somewhat better positioned, having solutions in place for:

- Application security
  (72% members, 59% industry professionals)
- Disaster recovery/business continuity
  (67% members, 62% industry professionals)

American Institute of Aeronautics and Astronautics
12700 Sunrise Valley Drive, Suite 200, Reston, VA 20191-5807 I 703.264.7500 I aiaa.org

Cybersecurity Beginning to Be Incorporated in Some Processes

When it comes to managing supply chain, development, engineering, and production processes, the aerospace sector has begun to incorporate cybersecurity considerations, but there is more to do.



- There is most likely to be a formal, structured process for incorporating cybersecurity considerations into ongoing operations and maintenance (76% members, 69% industry professionals) and in engineering and design phases of projects (74% members, 74% industry professionals).
- The industry is much less likely to have incorporated cybersecurity into the earliest stages of a project or in managing the supply chain. Only about 6 in 10 have done so for:
  - The proposal/bid process (60% members, 65% industry professionals)
  - Developing the risk assessment matrix (61% members, 62% industry professionals)
  - Vetting suppliers/vendors (61% members, 64% industry professionals)

Interest is Strong for Increasing Cybersecurity Awareness and Understanding

Interest in aerospace-tailored programming, resources, and professional development on cybersecurity is strong.

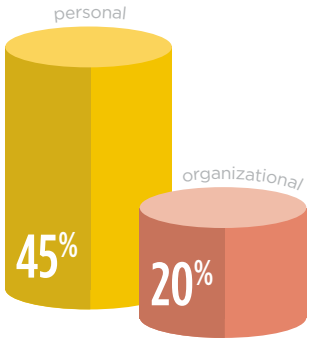
- Nearly three-quarters (73%) of members and 68% of industry professionals are interested in an AIAA cybersecurity program. Areas of unmet needs and greatest interest in AIAA developing content are:
  - Strategic and technical papers (72% members, 68% industry professionals)
  - Workshops and roundtables (72% members, 62% industry professionals)
  - Professional education and workforce development (69% members, 61% industry professionals)

Curriculum Development on Cybersecurity is Needed

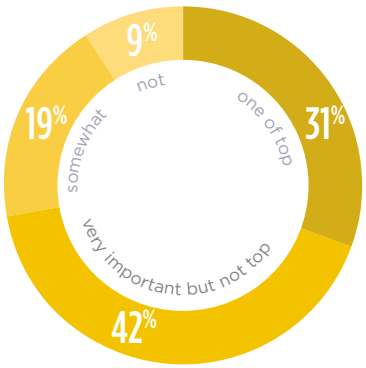
Looking ahead to workforce development and the young professional pipeline, there is strong interest in cybersecurity issues among academic partners, as well as support for developing aerospace cybersecurity curriculum. At the same time, they do not perceive commitment to this within their institutions.

- While 45% of academics say addressing cybersecurity challenges within the aerospace industry is a top priority for them, only 20% say it is a top priority for their organization or institution.
- Additionally, 31% say that having formal coursework in cybersecurity specifically for aerospace and related engineering disciplines is a top priority (73% top priority/very important) yet only 5% say there are specific cybersecurity course offerings for aerospace and engineering majors and only 26% say there is an option to take courses in another department that fits into the schedule at their college or university.
- Nearly three of four academics surveyed strongly support adding cybersecurity coursework specific to aerospace or related engineering degrees at their college or university (73% strongly/somewhat support).

Aerospace faculty see the importance of offering formal coursework in cybersecurity.



ACADEMIC FACULTY
% cybersecurity is top priority



IMPORTANCE OF OFFERING
FORMAL COURSEWORK

of academic partners support the addition of cybersecurity coursework specific to aerospace & related engineering

American Institute of Aeronautics and Astronautics
12700 Sunrise Valley Drive, Suite 200, Reston, VA 20191-5807 I 703.264.7500 I aiaa.org

New Cybersecurity Programming Planned by AIAA in 2021

AIAA is already developing dedicated forum and publication content that features integration of cybersecurity into aerospace engineering on par with safety and mission assurance. Future high-visibility cybersecurity content at AIAA forums and other events in the aerospace community will include:

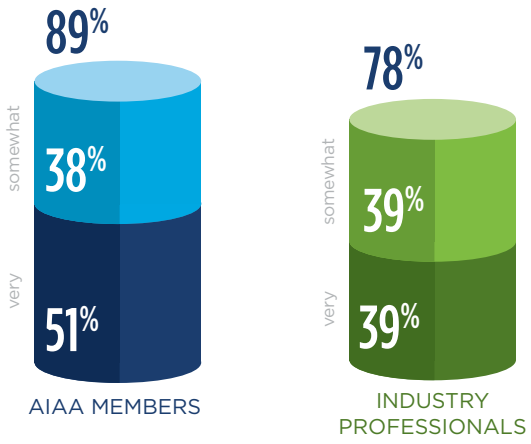
- Special interactive programming such as hacking contests or Capture The Flag competitions; and cybersecurity tabletop exercises for aerospace technical and business leaders
- Contributions from leading cybersecurity thinkers
- Participation in select non-AIAA events to expand programming to adjacent communities, such as the RSA and Defcon cybersecurity conferences

AIAA has already increased the frequency and amount of cybersecurity coverage in AIAA publications, including in Aerospace America, Daily Launch, and other AIAA media.

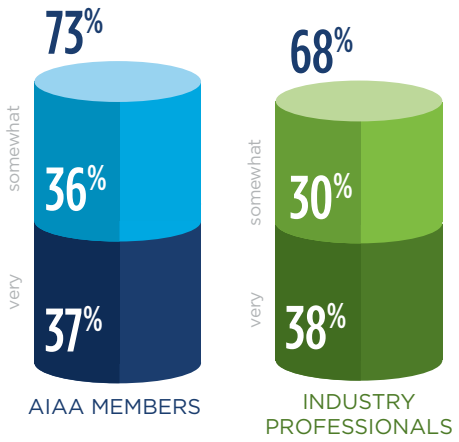
AIAA will offer a new aerospace cybersecurity course by the third quarter of 2021, designed to inform participants on such major issues at the nexus of aerospace and cybersecurity as emerging aerospace industry cybersecurity requirements, as well as vulnerabilities and protection measures specific to space and aviation systems.

AIAA's mission is to help our members be successful, and our cybersecurity program will help our members and the aerospace community meet the urgent new challenges of cybersecurity in aerospace. Recent national-level cybersecurity events and cyber threat trends, as well as emerging new cybersecurity requirements with impacts on aerospace, such as CMMC and SPD-5, underscore the need for leadership and resources equal to the new challenge. AIAA is working to bring relevant and impactful aerospace cybersecurity training, information, and event content that will advance aerospace cybersecurity and help our members succeed.

Most agree that AIAA should play a leadership role on cybersecurity for the aerospace industry.



Interest in an AIAA Cybersecurity Program is strong.



MOST DESIRED

- Strategic & Technical Paper Series
- Workshops & Roundtables
- Professional Education & Workforce Development

"It is becoming more and more essential to address cybersecurity on an ongoing basis in the mainstream of our core processes – from the design and development of new space systems to manufacturing and production to operations."

DAN DUMBACHER, Executive Director, American Institute of Aeronautics and Astronautics

ABOUT AIAA

The American Institute of Aeronautics and Astronautics (AIAA) is the world's largest aerospace technical society. With nearly 30,000 individual members from 91 countries, and 100 corporate members, AIAA brings together industry, academia, and government to advance engineering and science in aviation, space, and defense. For more information, visit www.aiaa.org, or follow AIAA on Twitter, Facebook, or LinkedIn.

American Institute of Aeronautics and Astronautics
12700 Sunrise Valley Drive, Suite 200, Reston, VA 20191-5807 I 703.264.7500 I aiaa.org