

Cyber Threats

The IFALPA Security Committee has identified the possibility of a cyber-attack against an aircraft, ground facility, or other critical infrastructure to be a significant threat that may cause unsafe situations or ultimately even loss of life. The purpose of this paper is to articulate this threat, and suggest ways in which it might be addressed.

OUR CONCERN

The typical commercial flight operation, whether passenger or cargo, generates and requires a large amount of data that is critical to the safe operation of the aircraft. Much of the technology currently in use was developed at a time when aircraft were relatively unconnected to the outside world, and therefore most of the systems are not designed to protect the information they carry. Furthermore, most communications between systems cannot be checked for integrity and completeness.

Cyber-attacks in society in general are very frequent. They can be carried out from virtually anywhere by anyone with sufficient knowledge, using low-budget methodologies. The goal of these attacks can be to obtain confidential, critical or sensitive information, to manipulate or erase information and/or to control or destroy systems or services. In many cases the compromised system may have not even been targeted but is taken down as a result of an attack elsewhere; in other words, it is a victim of “collateral damage”.

Therefore, cyber security should be considered throughout all aviation communications pathways and applications. This cannot be done by single entities for their own systems only. Due to the interdependencies in the realm of aviation, cyber security must be a shared responsibility of aircraft manufacturers, airlines, airports and air traffic control organisations together with their suppliers. Since public safety is at stake, States have the responsibility to make sure all parties involved take that responsibility.

REGULATIONS

States should establish regulations to set the minimum requirements that the aviation industry should meet. These could be specific technical cyber security measures, but preferably they would be outcome-based. Unlike physical security, cyber security techniques provide many ways to measure security performance, therefore a risk-based strategy is certainly an option.

Such regulations should not only provide technical requirements. Contingency planning is a very important aspect as well and should include proper training of all personnel that use safety critical systems to be able to detect actual cyber-attacks and act accordingly. Compliance should be audited by the authorities.

INFORMATION SHARING

In other industries information sharing has proven to be essential in the protection of critical infrastructure. In some countries structures have already been set up also for the aviation industry as well. If parties share information on security breaches, detected attacks and best practices the security of the system in total will benefit greatly. To be able to do that, confidentiality is key. Partners must be able to trust that the information will not be made public, until appropriate counter-measures have been implemented.

States should consider establishing a mandatory reporting system on aviation related cyber security incidents, again keeping confidentiality in mind. This would help in finding trends in threats, so appropriate measures can be taken when needed. It would also help in making sure all players in the aviation industry participate in the information sharing effort.

CONCLUSION

IFALPA considers the cyber issue to be a significant threat to the safety of aviation. It should be addressed in a coordinated manner without delay, both by the industry and by the regulators.

IFALPA BRIEFING LEAFLET ON CYBER THREATS

More detailed considerations about this subject can be found in a separate briefing leaflet published by IFALPA.

©2016 The International Federation of Air Line Pilots' Associations

IFALPA provides this data for information only, in all cases pilots should follow their company's guidance and procedures. In the interests of flight safety, reproduction of this publication in whole or in part is encouraged. It may not be offered of sale or used commercially.

All reprints must credit IFALPA.