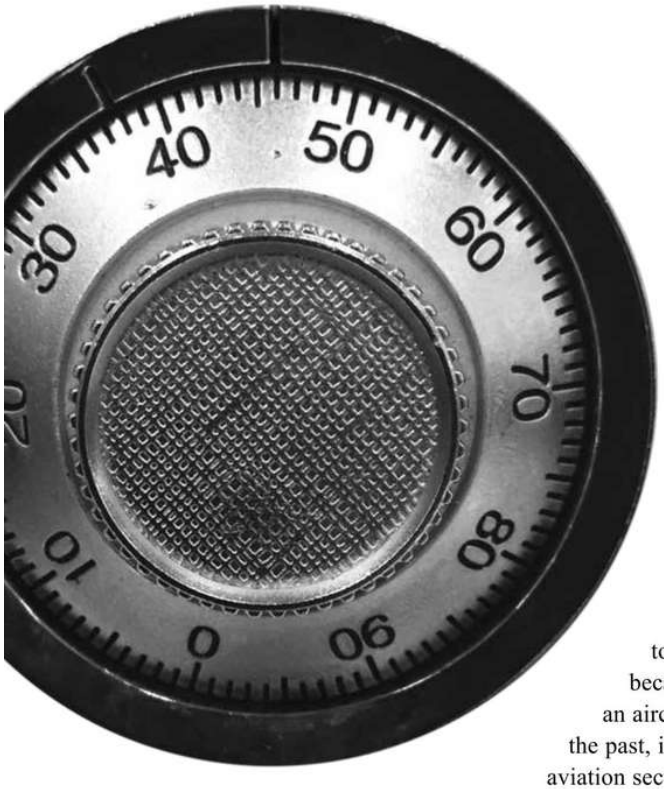
feature

GENERAL AVIATION SECURITY

How to develop a risk-based security plan



STORY BY LINDSEY MCFARREN

The Transportation Security Administration mandates security measures for many general aviation-related organizations, but not all. Some general aviation airports, businesses serving general aviation, aircraft operators, and others are left responsible for developing and implementing their own security measures. How should an unregulated organization develop a security plan?

The key is to know what risks your security program is mitigating. Not all aviation organizations are prime targets for terrorism. Threats to your organization might be in the form of theft, damage to expensive equipment, hacking of your network, or disgruntled former employee stealing your customer list.

Insider threat, defined by TSA as "one or more individuals with access to insider knowledge that allows them to exploit the vulnerabilities of the nation's transportation systems with the intent to cause harm," is fairly uncommon in general aviation; however, because general aviation insider smuggling of illicit drugs or use of an aircraft to commit suicide or otherwise cause damage has occurred in the past, insider threat mitigation methods should be included in any general aviation security plan.

Read on for more about the current regulatory environment, resources provided by several industry and government resources, and some general guidance for developing your own security plan.

Regulatory environment

First, consider the current regulatory environment for general aviation operators, airports, repair stations and other vendors to the general aviation industry.

Earlier this year, the TSA officially withdrew a proposed rule that would have established the Large Aircraft Security Program. The LASP would have mandated a number of security policies and procedures for general aviation operations of aircraft weighing more than 12,500 pounds and certain airports those aircraft use.

In 2014, the TSA finalized the Aircraft Repair Station Security rule, which requires certain repair stations (i.e., those located on a Part 1542 airport, or one that serves commercial aircraft) to have a security program that meets the rule's requirements. If your organization is subject to this rule, you are probably already complying with many aspects of a repair station security program.

Currently, non-airline operations are primarily regulated by the Twelve-Five Standard Security Program, Private Charter Standard Security Program, and the DCA Access Standard Security Program, which apply to large aircraft (more than 12,500 pounds maximum takeoff weight), and the Alien Flight Student Program that applies to smaller aircraft used at flight training facilities.

However, these rules do not apply to the entire general aviation community and a one-size-fits-all approach is just not appropriate for general aviation security, so industry and government partnerships have developed guidelines for general aviation organizations looking to establish their own scalable, voluntary security programs.

Industry and government resources

Industry and regulators have developed resources for general aviation operators and businesses to implement security plans.

Does your organization participate in the Aircraft Electronics Association's Safety Management System? The internal audit process, as part of the SMS, includes a security-based module. Organizations can use that module as guidance to develop simple but effective security measures.

The Aviation Security Advisory Committee is a government/industry group of TSA and industry representatives. It includes a general aviation subcommittee, which recently updated the "Security Guidelines for General Aviation Airport Operators and Users" to reach beyond the original audience of general aviation airports and include more of the general aviation industry. The guidelines now provide aircraft owners and pilot, airport operators, and other members of the general aviation community recommendations on establishing security programs.

INDUSTRY AND REGULATORS HAVE DEVELOPED RESOURCES FOR GENERAL AVIATION OPERATORS AND BUSINESSES TO IMPLEMENT SECURITY PLANS.

The guidelines encourage the use of risk-based security measures. Risk-based security begins with an assessment of threats, vulnerabilities, and consequences, and ensures resources are focused on areas where security measures might have real impact to mitigate risks.

The guidelines describe eight signs of terrorism, which can be used in training employees of general aviation businesses to raise awareness. The government/industry group also identified a number of security enhancements appropriate to general aviation, some of which might be applicable to your organization.

Finally, the guidelines provide a template for a general aviation airport security program. Although geared toward airports, the outline of the template and some portions of the content may be applicable to your organization, whether a repair station, FBO or other service provider for general aviation.

The Aircraft Owners and Pilots Association's Airport Watch program should also be included in your security plan. The Airport Watch program relies on pilots and other airport users to report suspicious activities to authorities through a telephone hotline answered by federal authorities. Call 1-866-GA-SECURE if you see suspicious activity at the airport, and also encourage your employees to use the hotline.

FBOs and other vendors to the general aviation community can use the requirements of the International Standards for Business Aircraft Handlers, developed and managed by the International Business Aviation Council, for more guidance on establishing security measures.

Finally, some municipalities, states and local airport

Continued on following page

Continued from page 29

authorities have security requirements or guidelines for organizations located on an airport. Review these requirements and guidelines – even from other states or municipalities – and use the relevant guidance to develop your own program.

Elements of an effective security program

The tallest fence does not make the most-effective security program. As they say, show me a 6-foot fence and I'll show you an 8-foot ladder. Many general aviation businesses and airports equate giant fences and fancy surveillance equipment with the best security measures. The reality for most general aviation organizations is security doesn't need to be that complicated.

First, conduct a simple threat assessment. Is your organization based on a busy airport, but not subject to TSA-mandated security programs? Does your general aviation airport host thousands of transient aircraft operations every year? If so, your needs are different from a repair station located in an industrial park adjacent to a small general aviation airport or from a general aviation airport that hosts few transient aircraft operations and even those from small single-engine piston aircraft. The threat assessment of a seaplane base next to a marina is different from a large general aviation airport like Van Nuys in the Los Angeles area.

Your organization's threats might not be terrorism-based. Maybe your organization is located in a small town where bored kids do dumb things, like steal runway lights or spray graffiti on hangars. Know the threats to your organization and consider what measures are necessary to mitigate those threats.

The vulnerabilities of a specific general aviation organization depend on many variables, including types of aircraft operating on or near the airport; population of nearby cities; facilities nearby, such as power plants or military facilities; and so on. Use the security assessment in the TSA's "Security Guidelines for General Aviation Airport Operators and Users" to conduct an objective assessment relevant to your operation.

Next, use the results of the threat assessment for your organization to determine any gaps. Do you allow visitors into areas that should be for employees only? Has that door to the hangar with the lock that sticks ever been fixed? Is your risk level high enough to require background checks of all employees, not just verification of airman or mechanic qualifications for pilots and mechanics?

The gaps identified above will help determine the direction of your security plan.

Most general aviation organizations and vendors that serve them can benefit from some simple, low-cost security measures.

> ***Visitor sign-in*** – Require visitors to sign in upon entering your facility. This allows you to keep a record of each person entering and leaving the building, which is helpful not only from a security perspective but from a safety perspective. During a severe weather event like a tornado or a facility fire, it is useful to know who is in the building.

> ***IT practices*** – Establish policies related to network security, including control of passwords. Make sure employees are aware of threats related to phishing and can identify suspicious emails and hyperlinks.

> ***Facility key control*** – Do all of your locks work properly? How many people have keys to your facility? If someone resigns or is fired, do you get their key back and/or re-key your doors?

> ***Aircraft key control*** – Keep aircraft keys secured and, if in an environment in which multiple pilots use one aircraft like a flight school or flying club, use a sign-out process for aircraft keys – each and every time.

> ***Employee background checks and badges*** – If you're in a TSA-designated Security Identification Display Area, this is covered for you. For everyone else, unless you're a three-person repair shop, consider employee background checks and simple badges. Identify sensitive areas like hangars and work rooms as employee-only, badge-required areas. Not only is this a good security measure, it keeps visitors safe from dangerous equipment – and keeps your sensitive, expensive equipment safe from visitors!

> ***Security training*** – Conduct basic security training for your employees. It doesn't need to be complex or lengthy but should include an overview of your security plan; emphasize "if you see something, say something;" and remind employees whom to contact in the event of a security breech or suspicious activity. Instruct employees to be watchful for potential signs of insider threat, such as personality changes or suspicious behaviors from colleagues, flight students, and other airports users. The main goal of general aviation security training is simply awareness.

Use the resources above to develop a security plan appropriate to your organization and the relevant risks. Document your plan, train your employees, and be consistent in your implementation. Any policy not followed or enforced isn't worth the paper you wrote it on, so be sure the security plan you develop makes sense for your organization. A simple, consistently implemented plan is far more efficient than a complicated and forgotten one. ❑