SECURITY MORE IMPORTANT THAN EVER AT FBOS

News / Business aviation

Our world is a dangerous place these days, with the threats of international and domestic terrorism mingling with more common hazards, such as vengeful ex-employees, vandals or other unhinged individuals. While some in the aviation service industry might ask *Why us?* , the answer is simple: private aviation by its nature attracts high-profile individuals such as celebrities or company executives, who in turn attract trouble from stalkers and paparazzi to corporate espionage, even eco-terrorism. An FBO must be prepared to deal with all of these threats, according to Randall Biglow, vice president of global operations with Washington, D.C.-based security consultancy At-Risk International.

There is currently no FBO security standard in the U.S. from a government perspective (aside from specific programs such as the DCA Access Standard Security Program for private aircraft heading into Washington Reagan National Airport). Biglow believes that in this day and age all FBOs must receive risk assessments and security surveys to transform themselves into “hard” targets, to protect their clients and their businesses. While this might evoke the image of a facility bristling with artillery and foot-thick walls, a more accurate picture blends technology and the human element that monitors it, and shows where the security can be bolstered.

MAKE THE MOST OF SECURITY TOOLS

For starters, Biglow noted that all employees at the company, from the president to the janitor, should receive situational awareness training so they will be more likely to notice, for instance, the

van that's been parked across the street for the past several days and alert authorities. "When you develop your situational awareness," he said, "you can discard the things around you that you don't need to focus on and identify the things that are more important." Such an approach will help a company to be proactive–rather than reactive–in its security approach. "Everybody needs to be part of security," said Biglow. "If there is a security department or security officer, big deal; they just get to wear the tie and hat." All workers should be empowered to challenge anyone in the facility they do not recognize, without fear of consequence, and that protocol should be explained to customers and vendors to avoid misunderstandings.

Though many locations have installed modern security systems, Biglow believes few are used to their full potential. "A lot of companies put in these wonderful elaborate systems but they don't use the integration," he said. "Most of the systems today can interact and communicate." What that means is that a movement sensor in a camera can trigger it to start recording (with several seconds of buffered memory before the movement so as not to miss anything), while simultaneously turning on the lights and issuing an alarm either to the front desk or a security monitoring company.

Proper lighting, according to Biglow, is one of the most inexpensive and effective security measures. In addition to serving as a deterrent, lighting will enhance the use of camera systems. All instances where an alarm is triggered or a light sensor activated should initiate some sort of immediate response from the company, to show someone is indeed monitoring, in case a wrongdoer is trying to probe the security system.

For access control, Biglow prefers card readers to keypads, as it is difficult to keep track of who has the door code. A properly configured security system can not only identify which card is used to open a door, but also if it belongs to someone who normally does not have access at that time of day (or night); if that is the case it can send an alerting text or email or even trigger an alarm or activate the camera system.

When it comes to determining your security needs Biglow offers this advice: "You don't want to have your technology installation person or company do your risk assessment, and you don't want them to design your system before the consultant gives them the specs." In many cases, he noted, the technology provider will try to sell you the equipment they want to sell you rather than what you need. Lastly, the specifications from the security consultant should be enough for an equipment provider to design a security system, without any further cost. "If you are paying for a security technology system to be designed for your company, shame on you; you're throwing away money," said Biglow. "Your installation company wants to sell you the equipment and install it and monitor it. Don't pay them to design the system."

17 MARCH 2016

SOURCE: AIN
ARTICLE LINK:
https://50skyshades.com/index.php/news/business-aviation/security-more-important-than-ever-at-fbos