Cybersecurity seen as rising risk for airlines after 9/11

September 11 2021, by Juliette Michel

Twenty years after 9/11, airlines are increasingly focused on cybersecurity risk.

After remaking their security procedures following the 9/11 attacks to stop airline hijackings, carriers are now faced with rising threats targeting computers and electronic equipment critical to their operations

and safety.

Since the tragedy 20 years ago on Saturday, airlines and airports have fortified cockpits, barred sharp objects in carry-on luggage and improved technology to detect explosives.

"We are more secure," said Willie Walsh, director general of the International Air Transport Association.

Many of today's security risks are now viewed as targeting the networks and hardware planes and airlines rely on.

From the gradual shift to electronic tickets to the management of jet fuel, even more aspects of aviation go through digital channels now than they did two decades ago.

"We must stay ahead of emerging security threats," Walsh said. "To do this effectively, we need to take a more integrated approach on things like cyber risks, drones, and insider threats."

New entry points

Beyond new airline security rules mandated by governments worldwide, security experts say potential hijackers face an additional challenge: other passengers.

"Because of 9/11, if you're sitting in the airplane, and someone jumps up and tries to enter the cockpit, the passengers themselves are going to fight back and prevent that from happening," said Dan Cutrer, an expert in aviation safety at Embry-Riddle Aeronautical University.

However the embrace of digital technology has created new opportunities for trouble, with hackers able to penetrate systems through

suppliers' software, online services or WiFi offered to passengers.

Experts consider the potential for a hacker to take control of the plane itself as unlikely, since flight controls are separate from systems used by customers.

Even if plane systems "may exhibit cybersecurity weaknesses, they're not an attractive target for most actors because of the required access and expertise, plus the risk of loss of life," said Katelyn Bailey of cybersecurity company FireEye.

A realm of potential vulnerability is the communication system between pilots and air traffic controllers, said Pablo Hernandez, a researcher at Innaxis Research Institute.

The conversations "are open and they're not encrypted or confidential," he said. "Anyone with the right radio can join into this conversation."

However, key flight systems needed to run the plane and air traffic have been well secured, Hernandez said.

There have been some notable hacks of ground or ancillary systems, including a 2020 data breach at British airline EasyJet that exposed the personal data of some nine million customers.

There were 1,260 incidents last year against airlines and other aviation bodies, such as airports, according to Eurocontrol, an intergovernmental organization that supports European aviation.

"Every week, an aviation actor suffers a ransomware attack somewhere in the world, with big impacts on productivity and business continuity," Eurocontrol said in a note published in July.

Airports use "best practices" to try to mitigate this risk.

This includes sending employees fictitious emails with links such as the ones devised by hackers; workers who click on them then receive additional training, said Christopher Bidwell, senior vice president at the Airports Council International, North America.

Money and espionage

The implications of cyberattacks are significant for airlines.

"In the aviation industry, you can't have downtime," said Deneen DeFiore, chief information security officer at United Airlines. "Any system outage or disruption would be detrimental to any company."

Most hackers are motivated by money. They use or sell stolen credit card data or financial information and sometimes demand ransom from companies to recover their systems.

However Bailey of FireEye said that because they often target the data of passengers, some hackers may be connected to states and engaged in espionage.

The airline industry benefited from the 2014 creation of an information sharing body, Aviation ISAC, focused on cybersecurity, said United's DeFiore.

She considers cyberattacks an emerging risk throughout aviation that needs to be taken seriously by everyone from air safety directors to maintenance teams.