Shanthan Kumar Bine
991447982

Case Study 7.1

1. **In your opinion, which of the two aircraft breaches is more dangerous: the breach described here, or the breach created by the hacker (described earlier in the chapter) who took control of a plane's throttle briefly through the entertainment system and then tweeted about it? Why?**

A. It's challenging to choose which of these highly dangerous air breaches is the most serious, but in my opinion, the hacker taking over a plane's thrust control is the worst-case scenario. The second attack involved sending phony flight plans to a variety of different aircraft, but the crew's approval is what matters most. Using a printed paper route that has the same waypoints as their on-screen route, the flight crew can compare their on-screen route to the flight plan that was broadcast by ACARS.

Another level of confirmation can be added by having the crew get in touch with the flight services station and ask for the waypoints that were added to the flight plan. The crew should be able to recognize the fake flight plan if they are paying attention to their official flight plan as filed by the airline. But if the crew is unable to spot the fake flight plan, a collision could happen in the air. Air traffic control will try to divert other aircraft if they don't follow their field flight plan, but it's likely they won't be successful. The crew would be in danger if the hacker managed to take over the aircraft's thrust control. They would undoubtedly arrive at a safe landing if this occurred while they were sailing. The aeronautical stall would be catastrophic and unrecoverable if it happened during takeoff.

2. **What questions would you pose to the information security executive responsible for the flight plan system to ensure that this hack was no longer possible? What other plans would you put in place to build a defense in depth?**

A. I would like to question the information security executive in charge of the flight plan system these following questions:

- How did the business react and respond to the breach of the ACARS network?
- What security measures are being implemented right now to address the ACARS network's safety?

- What stage has the committee reached in developing the standard for a flight plan security and when is it expected to be put into implementation ?
- Who else can access the plan?
- How are the in-flight communication networks created and controlled in the state of an emergency or a change in the flight plan?
- Can a system recognize an uploaded and approved fake plan?

I'd suggest implementing the following tactics to build a solid defense:

- Conduct routine security audits and risk analyses of the ACARS network to identify vulnerabilities and decide which security measures to prioritize.
- Implement authentication processes, such as two-factor authentication or OTP, to ensure that only authorized personnel can access the ACARS network.
- End-to-end encryption of all communications on the ACARS network is required to thwart hacker surveillance and interceptions.
- Install intrusion detection and prevention systems to spot and thwart any unauthorized access attempts and breaches.
- To gain access to any private data that is kept on a protected network.

3. **If password control is used to solve the ACARS weakness, what might hackers do next? And given your answer, what might managers do to guard against that?**

A. If password control is used to fix the ACARS vulnerability, hackers might try to use social engineering methods like phishing or pretexting to steal passwords from authorized users. They might also attempt to exploit other ACARS network flaws, such as outdated software or improperly configured computers. Managers should require the following to protect against these risks:

- Workers should receive instruction on recognizing and preventing the release of private information due to phishing.
- Updates and bug fixes should be applied on a regular basis to keep all systems secure and up to date.
- Hold regular phishing simulation training to promote excellent security practices among all employees.
- Keep an eye out for any suspicious activity on the network and immediately detect and investigate any potential security breaches.