Discussion Questions

1. Which of the two aircraft breaches is more serious: 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?
2. Which of the access controls and storage/transmission controls would be most helpful for the ACARS problem? The entertainment system problem? Why?
3. If password control is used to solve the ACARS weakness, what might hackers do next?

Sources: Kim Zetter, "All Airlines Have The Security Hole That Grounded Polish Planes," *Wired* (June 22, 2015), http://www.wired.com/2015/06/airlines-security-hole-grounded-polish-planes/ (accessed August 25, 2015); and "Hackers Ground 1,400 Passengers at Warsaw in Attack on Airline's Computers," *The Guardian* (June 21, 2015), http://www.theguardian.com/business/2015/jun/21/hackers-1400-passengers-warsaw-lot (accessed June 26, 2015).

■ CASE STUDY 7-2 Sony Pictures: The Criminals Won

The Tech section in *Forbes* magazine reported that the "criminals won" in the Sony pictures breach. An anonymous threat posted on an obscure site warned that people who watch the to-be-released movie *The Interview* would be "doomed" to a "bitter fate" and recalled the tragic events of September 11. The threat said that the movie inappropriately made light of North Korean officials.

As a result of the threat, five large theater chains in the United States and Canada canceled plans to include the film on their screens. Ultimately, Sony had no choice but to cancel the theater release of the film for reasons that are both economic and legal. The former was due to a lack of revenue given the small number of remaining theaters that might go ahead and run the film. The latter was driven by what would happen if an attack was carried out. A Steve Carell project that featured North Korea was also canceled.

The Guardian reported that a group named the Guardians of Peace retaliated against Sony. They hacked into Sony's systems and stole over 100 terabytes of files, including unreleased movies, social security numbers for thousands of Sony employees, and internal e-mails, some of which show embarrassing conversations between Sony employees. The hackers began distributing the files in various locations online, making them free for the taking.

The officials of that government denied any involvement in the hack but said that it might have been a "righteous deed" of those who support the government.

North Korean officials demanded some changes to the movie, including taming down a death scene of its leader. Sony initially refused but then decided to go ahead and edit the scene. The movie eventually opened without incident on a limited basis in some cinemas on Christmas Day and then was made available via online rental.

According to the *Mirror* in the United Kingdom, neither the Department of Homeland Security nor the FBI could find evidence that the violence was a credible threat, but the FBI believed North Korea was behind the hacking. In turn, North Korea claimed that the U.S. government was responsible for creation of the movie.

Discussion Questions

1. Setting aside the political issues between North Korea and the United States, is there a reasonable way to respond to an anonymous threat found on the Internet somewhere? What elements would you require before canceling the film if you were CEO of Sony? If you were CEO of a chain of theaters?
2. What access and data protection controls would you recommend Sony use to provide better security for unreleased digital films and e-mails?
3. If you were a hacker, what approach would you have used to break into Sony's system? What do you think the most important SETA elements would be to prevent future hacker attacks against Sony or other media firms?

Sources: Dave Lewis, "Sony Pictures: The Data Breach and How the Criminals Won," *Forbes Tech* (December 17, 2014), http://www.forbes.com/sites/davelewis/2014/12/17/sony-pictures-how-the-criminal-hackers-won/ (accessed June 25, 2015); Oliver Laughland, "The Interview: Film at Center of Shocking Data Breach Scandal Opens in LA," *The Guardian* (December 12, 2014) http://www.theguardian.com/film/2014/dec/12/the-interview-sony-data-hack (accessed June 25, 2015); and Anthony Bond, "Sony Hack: The Interview WILL Be Released Despite Huge Cyber Attack Against Film Maker," *Mirror* (December 23, 2014), http://www.mirror.co.uk/news/world-news/sony-hack-interview-released-despite-4868965 (accessed June 25, 2015).