University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 1

CS 4950/5950
Homeland Security & Cybersecurity

Lesson 30
Aviation Security
Exercise 1

Rick White, Ph.D.
University of Colorado, Colorado Springs

1
Esc

1

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 1

Let us begin by considering the different challenges posed by maintaining a mobile asset, in this case an aircraft, compared to a fixed asset such as a water plant.

2
Esc

2

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 1

- **Question 1.** Let us say that you receive a patch for a control system in a water plant.
- How many control systems do you suppose you have to update?

3
Esc

3

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 1

- **Answer 1.** Probably only one. A couple at most.
- One plant, one system.

4
Esc

4

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 1

- **Question 2.** Let's say you receive a patch for a particular aircraft avionics suite.
- How many aircraft do you have to update?

5
Esc

5

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 1

- **Answer 2.** All of them. That could mean many dozens.

6
Esc

6

TR Exercise 1

- **Question 3.** Returning to the water plant.
- How soon from the time you receive the patch until you can install it on your control system?

7

TR Exercise 1

- **Answer 3.** As soon as possible. Immediately if necessary.

8

TR Exercise 1

- **Question 4.** Now back to the avionics upgrade.
- How soon from the time you receive the patch until you can install it aboard all affected aircraft?

9

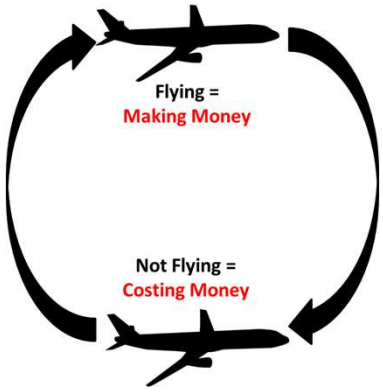
TR Exercise 1

- **Answer 4.** The answer's the same: as soon as possible; immediately if necessary.
- **The difference is the patches can only be made when the aircraft can be taken out of service.**

10

TR Exercise 1

- **An aircraft that is not flying is not making money.**
- Accordingly, the patch won't likely be installed until the next scheduled maintenance period.
- **This could have its own consequences.**



TR Exercise 1

- **Question 5.** Back to the water plant.
- What is the window of vulnerability to the threat fixed by this patch?

TR Exercise 1

- **Answer 5.** The window of vulnerability is from the time the patch is received until the control system is patched.

13

TR Exercise 1

- **Question 6.** Same question with respect to avionics.
- What is the window of vulnerability to the threat fixed by this patch?

14

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 1

- **Answer 6.** The window of vulnerability extends from the time the patch is received until the last aircraft is patched.
- This could be days if not weeks.
- **The window of vulnerability can be much longer for mobile assets compared to fixed assets.**

15

Esc

15

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 1

- **Question 7.** What is the risk to the water plant if the patch is not installed correctly?

16

Esc

16

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 1

- **Answer 7.** Possible service interruption.

17
Esc

17

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 1

- **Question 8.** What is the risk to the aircraft if the patch is not installed correctly?

18
Esc

18

TR Exercise 1

- **Answer 8.** Possible life safety.
- Disrupting the water supply is pretty serious.
- **Disrupting an aircraft's flight controls is even more serious.**

19

TR Exercise 1

- **Question 9.** What is the cost if the patch needs to be immediately installed at the water plant?

20

TR Exercise 1

- **Answer 9.** Possible service interruption.

21

TR Exercise 1

- **Question 10.** What is the cost if the patch needs to be immediately installed on all aircraft?

22

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 1

- **Answer 10.** Possible grounding of the entire fleet.
- **This could be a very expensive proposition.**

23
Esc

23

University of Colorado Colorado Springs

CS4950/5950
Homeland Security & Cybersecurity

TR Exercise 1

I hope you begin to see the difference between maintaining cybersecurity for a mobile asset compared to a fixed asset?

24
Esc

24

Conclusion

Questions?