Mar 3rd, 2:15 PM - 3:30 PM

Examining Pilot Response to Cybersecurity Events on the Flight Deck

Meredith Carroll Ph.D.
Florida Institute of Technology, mcarroll@fit.edu

Summer Rebensky
Florida Institute of Technology

Paige Sanchez
Florida Institute of Technology

Examining Pilot Response to Cybersecurity Events on the Flight Deck

Meredith Carroll, Summer Lindsey, Paige Sanchez

Cybersecurity in Aviation

- General focus of Cybersecurity: the systems
  - Hardening networks, Improving intrusion detections, Safe information sharing
- Little focus on human operator *(GAO, 2017)*

- Susceptibility to cybersecurity attacks increases in the aviation domain as technology such as electronic flight bags (EFBs) enter the flight deck *(Lundberg et al., 2014)*

GAO, Cybersecurity: Actions needed to strengthen U.S. Capabilities, GAO-17-440T (Washington, D.C., February 14, 2017)

Lundberg, D., Farinholt, B., Sullivan, E., Mast, R., Checkoway, S., Savage, S., Snoeren, A. & Levchenko, K. (2014). On the security of mobile cockpit information systems. *CCS'14*.

Goals of the Research

- Examine the human factors surrounding pilot detection of, and response to, a cybersecurity events on the flight deck
  - What factors influence detection and response?
  - Can pilots detect cybersecurity events?
  - How will they respond to a cybersecurity event?

ATLASLab Advancing Technology-interaction & Learning in Aviation Systems | FLORIDA TECH

Methods

1. Literature Review
2. Pilot Questionnaire
   - 108 Pilots: 60 airline, 30 corporate, 18 GA
   - Majority over 2500 flight hours
   - Perceptions of, experience with, and response to cybersecurity events on the flight deck
3. Simulation Study
   - 36 Boeing 737 Pilots
   - 7 Scenarios, 1 Cybersecurity event
   - Measures
     - Pilot decision making: Behavioural Checklist
     - Pilot Perceptions and Reactions: Questionnaire/Interviews

Literature Review

350 Abstracts

45 Publications

27 Relevant Publications

3 Aviation
4 Network Security
8 Personal Computing
8 General
4 Corporate Information Security

Pilot Questionnaire

Simulation Study

ATLASLab Advancing Technology-interaction & Learning in Aviation Systems | FLORIDA TECH

Literature Review Results: Cybersecurity Decision Process Stages

Susceptibility

An individual's perceptions/attitudes towards likelihood to experience a cybersecurity attack; trust in the systems, and subsequent behaviors to prevent attack.

Detection

Distinguishing system processes/ behaviors that are indicative of cybersecurity attack from normal activity.

Response

Response to a cybersecurity attack; how an individual decides to respond.

Literature Review Results: Influencing Factors

Stage		Susceptibility	Detection	Response
# of Supporting Studies		14	9	6
Factors Influencing Decision Process	Perceived Susceptibility	✕	✕	✕
	Perceived Safeguard Cost/Effectiveness	✕		✕
	System Trust	✕		
	System Reliability	✕		
	System Knowledge	✕	✕	
	Cybersecurity Knowledge/Experience	✕	✕	✕
	Saliency of Cybersecurity Event		✕	
	System Transparency		✕	

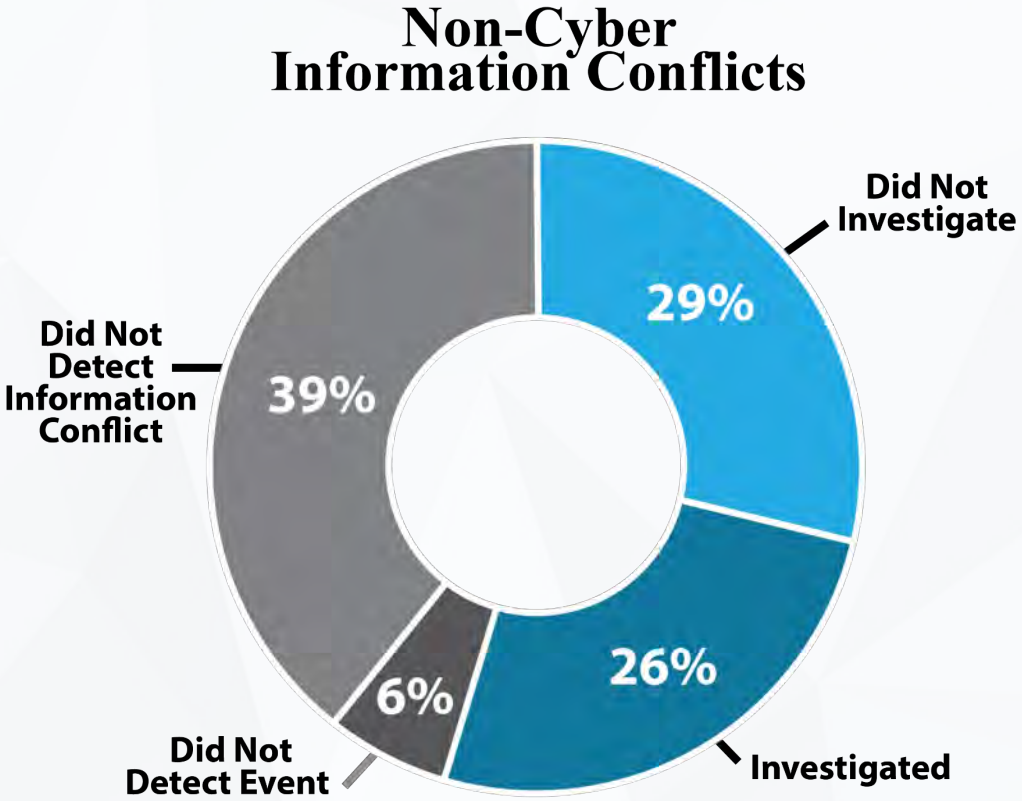
Questionnaire Results: Susceptibility to Cybersecurity Events

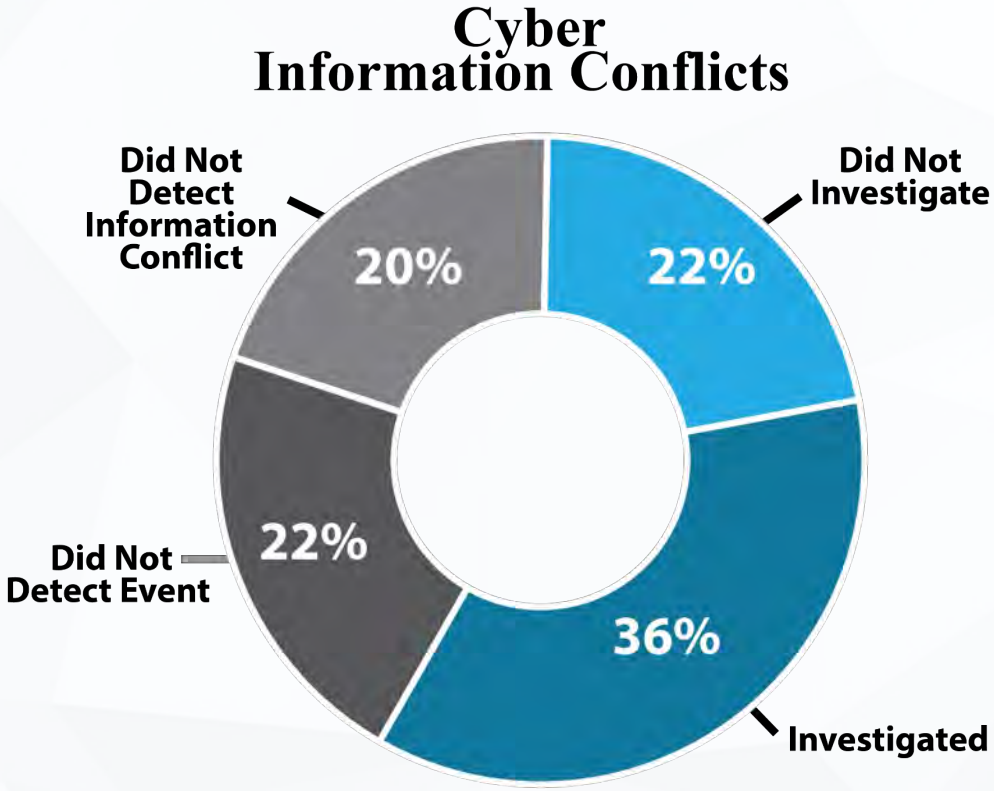
- Perceived Susceptibility
  - 78% of pilots thought EFBs or flight deck systems are vulnerable
  - Pilots appear to have moderate to high levels of perceived susceptibility for EFB systems compared to flight deck systems
  - 50% of pilots report using EFB for personal use
- Trust
  - 89% of pilots expressed moderate to complete trust in their flight deck information
- Safeguard Cost
  - Only 54% of pilots would be willing to use EFB solely for flight/company business
  - 23% wanted to continue personal use
  - 23% were willing to limit to company use or issued an EFB only during flights
- Cybersecurity Knowledge
  - Only 4 pilots of the 108 had received any SOPs or training on cybersecurity
  - Only 5 pilots of the 108 had received training

Questionnaire Results: Cybersecurity Detection and Response

- Only 4 of 108 pilots reported experiencing what they thought was a cyber event
  - Three of these were pilots who received training or SOPs on cybersecurity
- The 4 pilots who experienced what they believe to be a cybersecurity event responded similarly to other abnormal behavior on the flight deck
  - Overriding automatic processes
  - Alerting ATC/Dispatch
  - Landing at nearest airport
  - Using encrypted data
- Pilots who did not experience an event were asked how they believe they would respond
  - Responses were similar to actual responses reported

Simulation Study Results: Pilot Response to Cyber and Non-Cyber Events

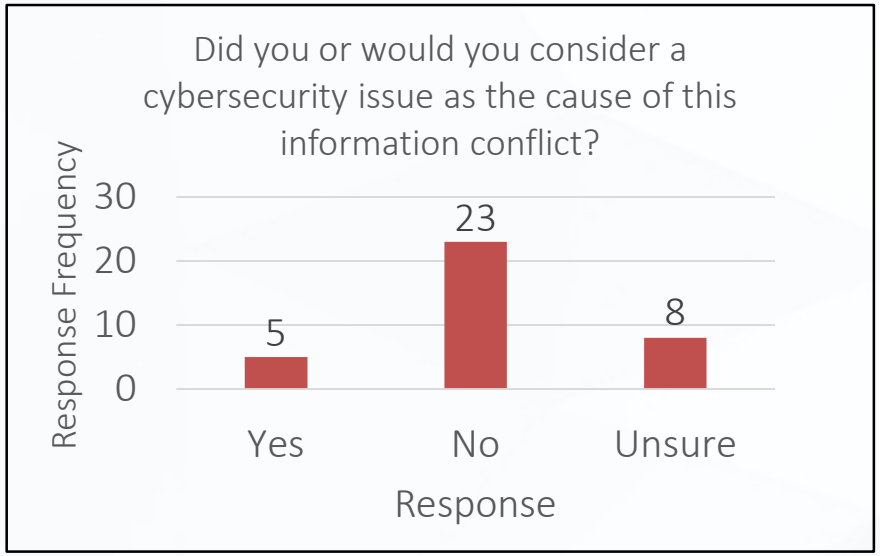




ATLASLab | FLORIDA TECH

Simulation Study Results: Participant Cybersecurity Perceptions

- 1 participant (3%) cited possible cybersecurity issue before priming
- 5 participants (14%) thought the information conflict could have been due to a cybersecurity event when specifically asked
- 4 participants (11%) had received training or SOPs on flight deck cybersecurity



Response	# Responses
Pilots would not be able to detect a cyber-attack	9
Maintain SA and monitor any change on displays	5
Crosscheck between multiple devices and displays	4
Consider last crew input on traffic display	2
Monitor EFB usage, unusual emails, notifications	2

1 Reason when asked "How could you know a cyber-attack is occurring on your cockpit displays?"

Trust and Concern Level for Flight Deck Systems and EFB

Flight Deck Trust

- "I never (or rarely) have an issue or experience to question trust in the systems
- "Systems onboard would be difficult to hack or compromise"
- "We have standby instruments and ways to verify information"

EFB App Trust

- "I've experienced issues with the programs [on the EFB]" such as "inaccurate or wrong data"
- There's a potential for "privacy issues and hacking"
- It's an "external source that is a backup to onboard systems"

- **High levels of trust** in both systems
  - Slightly higher for Flight Deck
- **Low levels of concern** with respect to information security of data
  - Slightly lower for Flight Deck

System	Trust Level	Concern Level
Flight Deck Systems	*4.67*	*1.50*
EFB Application	*4.19*	*1.83*

Note: average results based on 5-point Likert scale with 1=not at all, 5= completely or extremely

ATLASLab Advancing Technology-interaction & Learning in Aviation Systems | FLORIDA TECH

Implications

- Cybersecurity threats are not on pilots “radar”
- Pilots appear to respond to cybersecurity events in the same manner as to system anomalies
  - Likely because they are perceived as anomalies
- This is not necessarily a bad thing
  - Pilots currently do not receive training and do not have expertise in cybersecurity response
  - As a result, best response may be to treat as any other anomaly and follow procedures

Acknowledgement

This research was sponsored by the Federal Aviation Administration
NextGen Human Factors Division (ANG-C1)
under Contract # DTFAWA-16-D-00003.

ATLASLab Advancing Technology-interaction & Learning in Aviation Systems | FLORIDA TECH

Questions?

Dr. Meredith Carroll

Associate Professor, Aviation Human Factors

mcarroll@fit.edu

ATLASLab
Advancing Technology-interaction & Learning in Aviation Systems

FLORIDA TECH