วารสารวิชาการศรีปทุม ชลบุรี
ปีที่ 21 ฉบับที่ 4 เดือนตุลาคม ถึง ธันวาคม 2568

ความมั่นคงและปลอดภัยทางไซเบอร์ในระบบการบินยุคใหม่: การวิเคราะห์ความเสี่ยงและแนวทางป้องกัน

CYBERSECURITY AND SAFETY IN MODERN AVIATION SYSTEMS: RISK ANALYSIS AND PREVENTION APPROACHES

จิตลดา ปิยะทัต*

Jitlada Piyatat*

สาขาการจัดการธุรกิจการบิน คณะวิทยาการจัดการ สถาบันการจัดการปัญญาภิวัฒน์

Aviation Business Management Program, Faculty of Management Sciences,

Panyapiwat Institute of Management

*Corresponding Author e-Mail: jitladapiy@pim.ac.th

(Received: 2025, July 17; Revised: 2025, September 4; Accepted: 2025, September 12)

บทคัดย่อ

อุตสาหกรรมการบินในยุคดิจิทัลพึ่งพาโครงข่ายข้อมูลแบบเรียลไทม์ ตั้งแต่ระบบนำร่องผ่านดาวเทียมไปจนถึงแพลตฟอร์มวิเคราะห์การดำเนินงานภาคพื้น ซึ่งช่วยยกระดับประสิทธิภาพและความยืดหยุ่นของการปฏิบัติการ อย่างไรก็ดี ช่องโหว่ไซเบอร์กลับขยายตัวรวดเร็วจนมาตรการป้องกันแบบเดิมไม่เพียงพอ อุตสาหกรรมการบินยุคดิจิทัลต้องพึ่งข้อมูลแบบเรียลไทม์ จึงเสี่ยงต่อภัยไซเบอร์มากขึ้น แนวคิดหลักคือใช้ NIST CSF 2.0 เป็น “แผนที่ใหญ่” ว่าองค์กรควรรู้จักทรัพย์สินสำคัญ ป้องกัน เฝ้าระวัง ตอบสนอง และฟื้นตัวจากเหตุไซเบอร์อย่างไร

บทความวิชาการนี้จึงสังเคราะห์ภาพรวมความเสี่ยงไซเบอร์ตลอดห่วงโซ่การบินตั้งแต่อากาศยาน ระบบจัดการจราจรทางอากาศ ท่าอากาศยาน และห่วงโซ่อุปทานซอฟต์แวร์ นอกจากนี้ยังรวบรวมแนวทางป้องกันจากมาตรฐานสากลที่สำคัญ ที่อ้างอิงจากกรอบสากลงานเฉพาะทางการบินให้เทียบกับมาตรฐานสากลที่มีอยู่แล้ว ได้แก่ ICAO A41-19, NIST SP 800-82 Rev.2 และ EASA Easy Access Rules 2024 ในบทความยังอภิปรายประเด็นความรับผิดชอบเชิงเขตอำนาจ ความสอดคล้องของกฎระเบียบ การกำกับดูแลข้ามพรมแดน และภาวะขาดแคลนบุคลากร ซึ่งรายงานจาก International Information System Security Certification Consortium, Inc. เป็นสมาคมวิชาชีพไม่แสวงกำไรด้านไซเบอร์ซีเคียวริตี้ที่ก่อตั้งในสหรัฐอเมริกา เมื่อปี ค.ศ.1989 เป้าหมายหลักคือ “สร้างโลกไซเบอร์ที่ปลอดภัย” ISC2 ระบุว่าช่องว่างแรงงานไซเบอร์ทั่วโลกยังเกิน 5 ล้านตำแหน่ง ท้ายที่สุด เสนอ แผนที่ถนนระยะสั้น-กลาง-ยาว เพื่อยกระดับภูมิคุ้มกันไซเบอร์ และเน้นย้ำให้ทุกฝ่ายบนหลักการนโยบายเป็นข้อกำหนดตรวจสอบได้ในยุโรป และ FAA ASISP ช่วย

ผลักดัน security-by-design ตามแนวปฏิบัติ Aircraft Systems Information Security (ASISP) ซึ่งเป็นกรอบข้อกำหนดด้านไซเบอร์ซีเคียวริตี้สำหรับระบบอากาศยานของ Federal Aviation Administration (FAA) ของสหรัฐอเมริกา มีวัตถุประสงค์เพื่อส่งเสริมการรายงานและแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์ที่เกี่ยวข้องกับระบบการบินพลเรือนอย่างปลอดภัยและเป็นความลับ

คำสำคัญ: ความปลอดภัยไซเบอร์; การบิน; ดิจิทัล

ABSTRACT

The aviation industry in the digital age relies on real-time data networks, from satellite navigation systems to ground-based operational analytics platforms, which enhance operational efficiency and resilience. However, cyber vulnerabilities are rapidly expanding, rendering traditional defense measures inadequate. The digital aviation industry, relying on real-time data, is increasingly vulnerable to cyber threats. The key idea is to use the NIST CSF 2.0 as a "grand plan" for how organizations should identify critical assets, prevent, monitor, respond, and recover from cyber incidents.

This academic article synthesizes a comprehensive picture of cyber risks across the entire aviation supply chain, from aircraft, air traffic management systems, airports, and the software supply chain. It also aligns defense approaches from key international standards, drawing on the International Aviation Framework for Aviation, with existing international standards, including ICAO A41-19, NIST SP 800-82 Rev. 2, and EASA Easy Access Rules 2024. The article also discusses jurisdictional responsibilities, regulatory consistency, cross-border oversight, and talent shortages. The report is from the International Information System Security Certification Consortium, Inc., a nonprofit professional association specializing in cybersecurity founded in the United States in 1989. "Building a Safer Cyber World" ISC2 identified a global cybersecurity gap of over 5 million jobs. Finally, it proposed a short-, medium-, and long-term roadmap to enhance cyber resilience and emphasized policy principles for all parties as auditable requirements in Europe. The FAA ASISP helped promote security-by-design, following the Aircraft Systems Information Security (ASISP) guidelines, a cybersecurity framework for aircraft systems from the Federal Aviation Administration (FAA) of the United States. These guidelines promote the secure and confidential reporting and exchange of cyber threat information related to civil aviation systems.

Keywords: cybersecurity; aviation; digital

บทนำ

Global Navigation Satellite System (GNSS) เป็นคำเรียกระบบดาวเทียมต่าง ๆ ทั่วโลก ระบบเหล่านี้ให้ข้อมูลตำแหน่งและเวลาที่แม่นยำและเชื่อถือได้ทางการบินปัจจุบันนี้ได้มีการพัฒนาระบบนำทางด้วยดาวเทียมขึ้นมาหลายระบบ เช่น GPS (USA) GLONASS (Russia) Galileo (Europe) BeiDou (China), QZSS (Japan) SBAS ตลอดปี ค.ศ.2024 ผู้ควบคุมการบินแทบทุกภูมิภาคเริ่มชินกับสัญญาณเตือน “LOSS OF GNSS” ที่ดังถี่ขึ้นบนจอเรดาร์ สาเหตุไม่ใช่เพราะเครื่องรับสัญญาณเก่า แต่เพราะมีการขัดขวาง (jamming) หรือปลอมแปลง (spoofing) สัญญาณดาวเทียมมากขึ้นกว่าเดิมไว้หลายเท่า ข้อมูลล่าสุดของสมาคมขนส่งทางอากาศระหว่างประเทศ (IATA) ชี้ว่าเที่ยวบินที่ได้รับผลกระทบจากเหตุเหล่านี้เพิ่มจาก 260,000 ไฟลต์ใน ค.ศ.2023 เป็น 430,000 ไฟลต์ใน ค.ศ.2024 หรือราวร้อยละ 62.00 ภายในปีเดียว (International Air Transport Association, Online, 2024) สาเหตุจากการเกิดขึ้นเนื่องจากอุปกรณ์รบกวนที่มีราคาไม่แพงเป็นภัยคุกคามโดยใช้เครื่อง jammer กำลังส่งไม่กี่วัตต์ที่ดัดแปลงจากอุปกรณ์เพียงตัวเดียวสามารถทำหน้าที่เป็นเครื่องรับ-ส่งสัญญาณได้หลากหลายย่านความถี่หรือเรียกว่า Software-Defined Radio Module (SDR) สามารถซื้อผ่านออนไลน์ได้ต่ำกว่าหนึ่งร้อยดอลลาร์ เช่น คนขับรถบรรทุกซื้อไว้ปิดตาเครื่องติดตามเพื่อเลี่ยงจ่ายค่าทางด่วน” กลายเป็นเรื่องปกติ เทคโนโลยีที่เคยสงวนให้ทหารจึงเปลี่ยนผ่านสู่ผู้ใช้ทั่วไปอย่างรวดเร็ว (Huntley, Online, 2024) หรือความขัดแย้งในยูเครน ตะวันออกกลาง และพรมแดนอินเดีย–ปากีสถาน ทำให้ฝ่ายทหารเลือก “ปิดตา” ดาวเทียมของคู่แข่ง ส่งผลพลอยกระทบมาถึงการบินพาณิชย์ (Plucinska, Insinna & Pearson, Online, 2024)

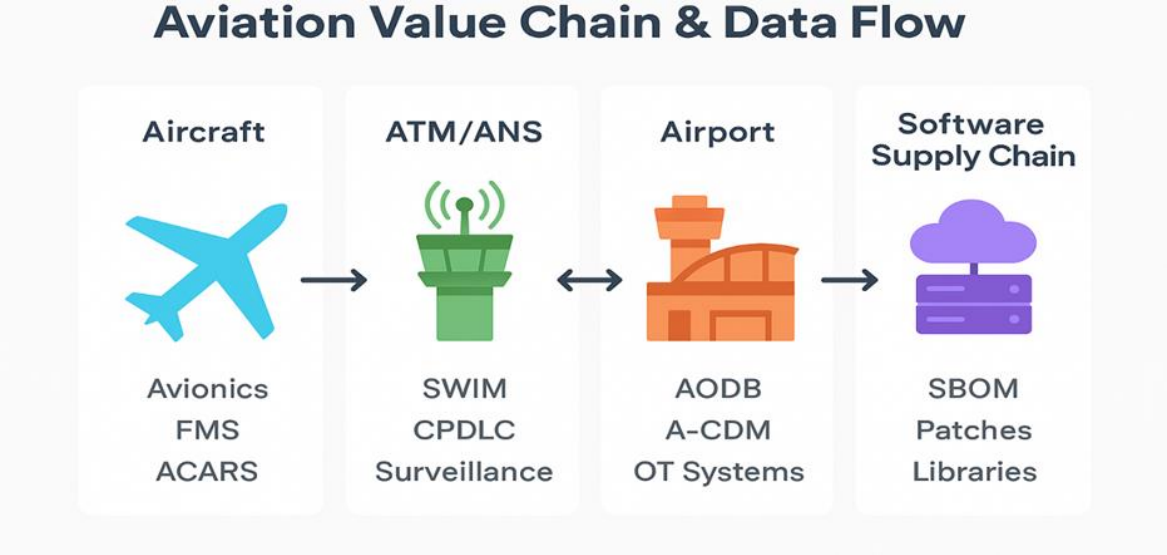
วัตถุประสงค์

1. เพื่อศึกษาและประเมินระดับความเสี่ยงไซเบอร์ขององค์ประกอบหลัก 4 กลุ่มอากาศยาน ATM/ANS ท่าอากาศยาน ห่วงโซ่อุปทานซอฟต์แวร์
2. เพื่อศึกษาและวิเคราะห์ระดับความเสี่ยงเชิงระบบมาตรการป้องกันเชิงเทคนิค-การจัดการ ตามเกณฑ์องค์การการบินพลเรือนระหว่างประเทศ (International Civil Aviation Organization: ICAO)
3. เพื่อศึกษาและประเมินผลกระทบจากภาวะขาดแคลนบุคลากร

ห่วงโซ่การบิน (aviation value chain)

อุตสาหกรรมการบินเป็นห่วงโซ่คุณค่าขนาดใหญ่ที่เชื่อมกิจกรรมตั้งแต่ต้นน้ำ—การออกแบบวิจัยพัฒนา และผลิตชิ้นส่วน/ระบบอากาศยาน—ไปจนถึงกลางน้ำ—การเงิน การเช่าเครื่องบิน การประกัน และการซ่อมบำรุง (MRO)—และปลายน้ำ—การให้บริการขนส่งผู้โดยสาร/สินค้า การบริหารท่าอากาศยาน การให้บริการจราจรทางอากาศ (ANSP) ผู้ให้บริการภาคพื้น ซัพพลายเออร์เชื้อเพลิงและครัวการบิน ตลอดจนแพลตฟอร์มการกระจายสินค้าและข้อมูล (เช่น GDS และผู้ส่งต่อสินค้าทางอากาศ) โครงสร้างเชิงเศรษฐศาสตร์

ของห่วงโซ่นี้มีผู้เล่นย่อยจำนวนมากและมีความเชื่อมโยงรายได้ข้ามเซกเตอร์สูง เช่น สายการบิน สนามบิน ผู้ให้บริการนำร่องทางอากาศ ผู้ให้บริการภาคพื้น ผู้ให้บริการ MRO ผู้เช่าเครื่องบิน ผู้จัดการกระจายสินค้า และผู้ผลิตเชื้อเพลิงปลายน้ำ (International Air Transport Association, Online, 2024; Lind, Saxon, Vik & Bouwer, Online, 2024).



ภาพที่ 1 Aviation Value Chain & Data Flow

ห่วงโซ่การบินเริ่มต้นบนฟ้า ณ จุดที่เครื่องบินกำลังลอยอยู่เหนือก้อนเมฆ อากาศยานจะรวบรวมสัญญาณ ตำแหน่ง ข้อมูลเครื่องยนต์ และข้อมูลผู้โดยสาร ส่งผ่านสัญญาณดิจิทัลลงสู่พื้นโลกแบบวินาทีต่อวินาที เข้าสู่ศูนย์ควบคุมจราจรทางอากาศ

ด้านบนคือ อินโฟกราฟิก Aviation Value Chain & Data Flow จัดวาง 4 ฟันเฟืองหลักของอุตสาหกรรมการบินจากซ้ายไปขวา 1) Aircraft ⟶ 2) ATM (Air Traffic Management)/ANS(Air Navigation Services) ⟶3) Airport ⟶ 4) Software Supply Chain พร้อมลูกศรแสดงการแลกเปลี่ยนข้อมูลแบบสองทาง

อากาศยาน (aircraft) ศูนย์ข้อมูลลอยฟ้า ที่เก็บ-สร้าง-ส่งเทเลเมทรี (การวัดค่าที่จุดหนึ่ง แล้วส่งข้อมูลนั้นไปยังอีกจุดหนึ่งเพื่อติดตาม วิเคราะห์ หรือควบคุมจากระยะไกล) สภาพเครื่อง และสถิติการบินแบบวินาทีต่อวินาที นำเข้าข้อมูลภารกิจจากภาคพื้นและผลักสถานะกลับไปยังศูนย์ปฏิบัติการเน้น avionics ซึ่งเป็นคำผสมระหว่าง “aviation” + “electronics” หมายถึงระบบอิเล็กทรอนิกส์ทั้งหมดบนอากาศยานที่ช่วยให้นักบินบังคับ ควบคุม นำร่อง สื่อสาร และตรวจตราสภาพเครื่องบินได้อย่างปลอดภัยและแม่นยำ ระบบบริหารการบิน (Flight Management System: FMS) คือคอมพิวเตอร์ศูนย์กลางบนอากาศยานที่ทำหน้าที่วางแผนจัดการและติดตามเส้นทางบินแบบอัตโนมัติ เช่น นักบินป้อนแผนการบิน คำนวณเชื้อเพลิงสำรอง ลดระดับ

การบินอัตโนมัติหรือแม้กระทั่ง ให้ระบบควบคุมบินทำงานเอง และติดตามตำแหน่ง พร้อมคำนวณพารามิเตอร์ เช่น น้ำหนักอากาศยาน อุณหภูมิ ความเร็วลม เนื่องจากเป็นส่วนสำคัญให้กับนักบินและระบบนำร่องอื่น ๆ ตลอดเที่ยวบิน ตั้งแต่ก่อนสตาร์ตเครื่องจนถึงขั้นตอนร่อนลงจอด ACARS (Aircraft Communications Addressing and Reporting System) คือระบบสื่อสารข้อมูลสั้น (datalink) ระหว่างเครื่องบินกับสถานีภาคพื้น

ระบบจัดการจราจรทางอากาศ (ATM/ATS) เสมือน “สมองส่วนควบคุมการจราจร” รับ-หลอม-กระจายข้อมูล ตำแหน่ง อากาศยาน-อากาศยาน และอากาศยาน-หอ เพื่อหอบังคับการบิน (ATC) สั่งทิศทางการบินให้เครื่องบินโดยตรง ด้วยตัวเลข ความสูง เช่น บินหัว 270 องศา เพื่อพาอากาศยานไปยังจุดหรือเส้นทางที่ต้องการอย่างแม่นยำและช่องทางบินให้ปลอดภัยและลื่นไหล

ท่าอากาศยาน (airport) เปรียบได้กับ “เมืองดิจิทัลขนาดกลาง” ที่ทุกวินาทีต้องจับคู่เที่ยวบิน-ประตู-สัมภาระ-ลูกเรือผ่านเครือข่าย เดียวกัน A-CDM (Airport Collaborative Decision-Making) เป็นกรอบแลกข้อมูล–ตัดสินใจร่วม ระหว่าง 4 หน่วยงานคือ ผู้บริหารสนามบิน (APO) หอบังคับการบิน (ATC) สายการบิน/ผู้ให้บริการภาคพื้น ทำให้หน่วยงานท่าอากาศยาน-สายการบิน-หอบังคับการบิน เห็นเวลาเดียวกัน ข้อดีคือ เพิ่มความแม่นยำของเวลาเที่ยวบิน และใช้ทรัพยากรรันเวย์-หลุมจอดเต็มประสิทธิภาพ ลดช่วงเวลาที่อากาศยานเคลื่อนที่จากหลุมจอดไปยังทางวิ่ง เพื่อเตรียมตัวขึ้นบิน (taxi-time) รวมถึงการใช้เชื้อเพลิง เป็นต้น

ห่วงโซ่อุปทานซอฟต์แวร์ (software supply chain) เป็นเบื้องหลังที่ส่งโค้ดและแพตช์เข้าสู่เครื่องบิน เซิร์ฟเวอร์สนามบิน และศูนย์ควบคุม ถ้าแพ็กเกจแค่หนึ่งไฟล์ถูกฝังมัลแวร์ ความเสี่ยงจะไหลไปทุกข้อของห่วงโซ่อย่างช้า ๆ

แนวโน้มภัยคุกคามและผลกระทบเชิงปฏิบัติการของ GPS jamming/spoofing

กรณีอากาศยานรุ่น A320 เที่ยวบิน FR748 จากเมืองริกาเข้าใกล้กรุงเวียนนาในสภาพฟ้าปิด นักบินเห็นไฟ GPS POSITION LOST ความหมายคือไม่สามารถคำนวณพิกัดจากดาวเทียม GPS สัญญาณจะกระพริบบนจอ พร้อมเสียงเตือนว่าเส้นทางไม่เสถียร สัญญาณนำร่องถูกรบกวน จนระบบ RNP-AR (Required Navigation Performance-Authorization Required) ใช้ต่อไม่ได้ จึงต้องยกเลิกการร่อนลงสองครั้งติดกัน แล้วบินอ้อมไปลงบรโน (Brno) สาธารณรัฐเช็กแทน ผู้โดยสารกางแผนที่ในมือถือพบว่าตัวเองอยู่ห่างกรุงเวียนนาร่วม 130 กิโลเมตร แม้จะปลอดภัยดี แต่สายการบินเสียค่ารถโค้ช ค่าเชื้อเพลิง และช่องเชื่อมต่อเที่ยวถัดไปทั้งแผง (IATA เรียกรายนี้ว่าเหตุการณ์ ‘minor tech issue’ ทว่ากระทบเที่ยวบินกว่า 180 คนเต็มลำ)

เมื่อเทียบกันใน 5 มิติหลัก ได้แก่ ความง่ายต่อการตรวจจับ,ลักษณะการเสื่อมของสมรรถนะการนำร่อง ภาระงานนักบิน ทางเลือกฉุกเฉินและพึ่งพาโครงสร้างพื้นฐาน ผลกระทบเชิงเครือข่ายและต้นทุน พบว่า jamming มักนำไปสู่ “การหยุดใช้ระบบกำหนดตำแหน่งและเวลาแบบอาศัยดาวเทียม” ที่ครอบคลุมทั่วโลก (GNSS) ทันที” นักบินและระบบสามารถรับรู้และสลับไปยังระบบวิทยุภาคพื้นให้ช่วยนำอากาศยานลงจอดแบบแม่นยำ แม้ทัศนวิสัยต่ำ (instrument landing system) ได้รวดเร็ว หากมีความพร้อมของอุปกรณ์/

โครงสร้างพื้นฐานในสนามบินปลายทาง ต้นทุนจึงมาในรูปของเวลาเพิ่ม ขีดความสามารถรันเวย์ที่ใช้ได้ และเชื้อเพลิงจากการวนรอ/ยกเลิกการร่อนลง ในขณะที่ spoofing ถึงแม้จะพบไม่ถี่เท่า แต่มี “ความเสี่ยงเชิงความปลอดภัย” สูงกว่า เพราะอาจทำให้ระบบเชื่อว่าตำแหน่งถูกต้องขณะคลาดเคลื่อน ดังนั้นภาระหลักอยู่ที่การตรวจจับเชิงขั้นตอนและเครื่องมือ

จากข้อมูลเห็นได้ว่ากรอบผลลัพธ์ด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร เข้ากับกรอบธรรมาภิบาลความเสี่ยง และมาตรฐานการบินสากล ให้ครอบคลุมทั้งด้านเทคนิค ขั้นตอน และการกำกับดูแล งานเดิมมักเน้นเทคโนโลยีสารสนเทศมากกว่าระบบควบคุมภารกิจและการจราจรทางอากาศ และพึ่งพาการนำร่องผ่านดาวเทียมเพียงอย่างเดียว โดยไม่ออกแบบการสลับไปใช้เครื่องช่วยลงจอดและวิทยุนำร่องภาคพื้นอย่างเป็นระบบ เมื่อนำมาใช้ในไทยพบข้อจำกัดเรื่องความพร้อมของเครื่องช่วยนำร่องภาคพื้นที่ต่างกัน โครงสร้างกำกับหลายหน่วย การแบ่งปันข้อมูลภัยคุกคามยังไม่เข้มแข็ง และขาดแคลนบุคลากรด้านความมั่นคงปลอดภัยของระบบควบคุมการบิน

จึงเห็นว่าควรจัดทำตารางเปรียบเทียบมิติสำคัญ (ขอบเขตภัย กลยุทธ์ควบคุม ธรรมาภิบาล เงื่อนไขสนับสนุน) แล้วกำหนดแผนระยะสั้น กลาง ยาว: ยกระดับวิธีบินสำรอง จัดทำข้อตกลงแบ่งปันข่าวสาร และกำหนด “ระดับความเสี่ยงที่ยอมรับได้” พร้อมพัฒนาบุคลากรเฉพาะทาง

กรอบกำกับระหว่างประเทศ

กรอบกำกับไซเบอร์ในระบบการบินสากลระหว่างประเทศ ไม่มีกฎหมายฉบับเดียวครอบคลุมทุกอย่างได้ แต่เป็นชั้น-ซ้อนของคำสั่งระหว่างรัฐบาล (ICAO) กฎระดับภูมิภาค เช่น EU และนโยบายของรัฐ/หน่วยงานกำกับ (FAA ฯลฯ) ที่ค่อย ๆ เชื่อมโยงเข้าหากัน ตัวอย่าง ICAO มติสมัชชา A41-19 (ปี ค.ศ.2022) กำหนดให้ไซเบอร์เป็นวาระด้านความปลอดภัยการบิน เช่นเดียวกับ safety เรียกร้องให้รัฐต่าง ๆ ผนวกการประเมินความเสี่ยงไซเบอร์เข้าในระบบกำกับดูแลโดยบังคับใช้ผ่านการปรับปรุง Annex 17 และคู่มือด้าน security

ระดับประเทศ/ภูมิภาค

สหรัฐอเมริกา FAA Cybersecurity Strategy 2020-2025 Federal Aviation Administration-FAA เป็นหน่วยงานที่รับผิดชอบด้านการบินแห่งชาติของสหรัฐอเมริกาอยู่ในสังกัดกระทรวงคมนาคม มีหน้าที่วางระเบียบและควบคุมตลอดจนตรวจสอบงานการบินพลเรือนของอเมริกาและยังเป็นผู้ให้คำแนะนำแก่หน่วยงานด้านการบินพลเรือนของประเทศต่าง ๆ ทั่วโลก ระบุในเอกสาร 10 หน้าของ FAA วาง 5 เสาหลัก (การกำกับ ป้องกัน-ตอบสนอง การจัดการความเสี่ยงด้วยข้อมูล บุคลากร ความร่วมมือภายนอก) ซึ่งใช้เป็นกรอบให้ Advisory Circulars เช่น ASISP บังคับผู้ผลิต-สายการบินระบุภัยไซเบอร์ตั้งแต่ขั้นออกแบบเครื่อง (FAA, Online, 2020)

สหภาพยุโรป ในอดีตองค์กรการบินแยก Safety Management System (SMS) กับ Information-Security Management System (ISMS) คนละสายงาน แต่ภัยไซเบอร์เริ่มลุกลามจากแค่ข้อมูลหายไปสู่เครื่องบินหลงพิกัด ทำให้สหภาพยุโรปออก Regulation (EU) 2023/203 บังคับให้องค์กรที่บินภายใต้ EASA ทุกประเภท-ตั้งแต่สายการบิน Part-145 ATC จนถึง U-space ต้องระบุ-ประเมิน-ควบคุม ความเสี่ยงด้านข้อมูลที่อาจกระทบความปลอดภัยการบิน ภายในกรอบ ISMS ของตัวเอง (European Commission, Online, 2023) Regulation (EU) 2023/203 และ EASA (European Union Aviation Safety Agency) องค์การความปลอดภัยด้านการบินแห่งสหภาพยุโรปจึงได้ออกกฎบังคับใหม่ Part IS (มีผลช่วงต้นปี ค.ศ.2025) ทุกองค์กรตั้งแต่โรงซ่อม ผู้ดำเนินการอากาศยาน Aircraft/ Airline Operator (AO) ผู้ให้บริการเดินอากาศ Air Navigation Service Provider (ANSP) จนถึงการจราจรทางอากาศดิจิทัลสำหรับอากาศยานไร้คนขับ U-space โดรน ต้องมี information-security management system เชื่อมโยงกับระบบ safety (EUROCONTROL, Online, 2025) เพื่อเพิ่มความปลอดภัยมากยิ่งขึ้น และยังมีตัวอย่างประเทศอื่นที่มีการใช้แนวทางเพื่อป้องกันควบคุม เช่น

GCAA (Online, 2024) กำหนดแนวทางบังคับไซเบอร์เป็นภาคผนวกของคู่มือตรวจ AOC (Air Operator Certificate) ใบรับรองผู้ดำเนินการเดินอากาศเพื่อยืนยันว่าผู้ครอบครองเอกสารใบรับรองนี้ผ่านการพิจารณาว่ามีความสามารถที่จะปฏิบัติการบินกับอากาศยานของตนได้อย่างปลอดภัย

สิงคโปร์-ไทย-ญี่ปุ่น เริ่มนำ ICAO Doc 10213 (International Civil Aviation Organization, Online, 2025) มาปรับในแผนนิรภัยในการบินพลเรือนแห่งชาติ (State Safety Programme: SSP) เวอร์ชันใหม่ เป็นต้น

ในระบบการบินยุคดิจิทัล บุคลากรด้านความมั่นคงไซเบอร์ได้กลายเป็นทรัพยากรขาดแคลนที่สุดชนิดหนึ่ง รายงาน CAE Talent Forecast คาดว่าทั่วโลกต้องการตำแหน่งใหม่สำหรับการบำรุงรักษาและความปลอดภัยของระบบสารสนเทศการบินกว่า 1.4 ล้านอัตราภายใน ปี ค.ศ.2034 (CAE, Online, 2025) ขณะที่ ISC2 ระบุว่าร้อยละ 67.00 ขององค์กรด้านความปลอดภัยไซเบอร์ยอมรับว่าขาดคนที่มีทักษะเฉพาะทาง (ISC2, Online, 2024) ภาคการบินจึงกำลังแข่งขันแย่งตัวผู้เชี่ยวชาญเดียวกันกับอุตสาหกรรมการเงิน คลาวด์ และพลังงาน

สาเหตุหลักแบ่งได้สามข้อ **หนึ่ง** โครงสร้างประชากร บุคลากรรุ่น baby boomer ในตำแหน่งนักบิน ช่างซ่อม และผู้ควบคุมจราจรทางอากาศทยอยเกษียณพร้อมกันหลังยุค COVID-19 แต่แรงงานรุ่นใหม่ยังอยู่ระหว่างการฝึกอบรม **สอง** คุณสมบัติด้านไซเบอร์ของการบินซับซ้อนกว่าปกติ ผู้เชี่ยวชาญต้องเข้าใจทั้งมาตรฐาน DO-178C กฎ Part-IS ของ EASA และแนวทาง Zero-Trust ทักษะชุดนี้ยังไม่มีในหลักสูตรมหาวิทยาลัยทั่วไป **สาม** งบประมาณบุคลากรท่าอากาศยานและสายการบินมักสู้แพ็กเกจค่าตัวจากบริษัทเทคโนโลยีใหญ่ไม่ได้ ส่งผลให้ตำแหน่งผู้เชี่ยวชาญที่ทำหน้าที่เฝ้าระวัง วิเคราะห์ และตอบสนองเหตุภัยคุกคามไซเบอร์ซึ่งอาจกระทบความปลอดภัยการบิน (Air-Cyber Analyst) หรือวิศวกรผู้ออกแบบ ติดตั้ง และดูแลโครงสร้างพื้นฐาน (Security Operations Center: SOC) ประกาศรับสมัครค้างไว้นานขึ้นเรื่อย ๆ

ผลกระทบเริ่มปรากฏชัดในงานปฏิบัติการ ท่าอากาศยานขนาดกลางหลายแห่งต้องเลื่อนการอัปเดตฐานข้อมูลศูนย์กลางของสนามบิน ใช้เก็บและกระจายข้อมูลเที่ยวบิน ตั้งแต่รหัสเที่ยว เวลา หลุมจอด ไปจนถึงสัมภาระ Airport Operational Database (AODB) ออกไปเพราะไม่มีวิศวกรที่ผ่านการรับรองระบบ OT ทำให้เสี่ยงต่อมัลแวร์เรียกค่าไถ่มากขึ้น ศูนย์ควบคุมจราจรบางแห่งแบ่งเวลาของผู้ตรวจสอบ safety มาช่วยตรวจเจาะ (pen-test) ระบบเครือข่าย SWIM (System Wide Information Management) เป็นโครงข่ายข้อมูลสากลของการบิน ที่ออกแบบให้ผู้เกี่ยวข้องทุกฝ่าย ตั้งแต่ศูนย์ควบคุมจราจรทางอากาศ (ATC) ท่าอากาศยาน สายการบิน นักบิน ไปจนถึงบริการอุตุนิยมวิทยาสามารถแลกเปลี่ยนข้อมูลผ่านมาตรฐานเปิดเดียวกันแบบบริการ-ต่อ-บริการ (service-oriented) แต่เนื่องจากไม่มี ผู้เชี่ยวชาญที่ทำหน้าที่ตรวจประเมินความมั่นคงไซเบอร์ (cyber-auditor) เฉพาะทาง ในระยะยาวหากช่องว่างทักษะยังคงอยู่ โครงการเสริมความทนทานของระบบนำร่อง (A-PNT) และศูนย์ปฏิบัติการไซเบอร์แบบรวมศูนย์ (Aviation SOC) จะชะลอตัวจนกระทบเสถียรภาพของทั้งเครือข่ายการบิน

ทางออกเบื้องต้นแบ่งได้สี่แนวทาง ดังนี้ 1) ขยายต้นทาง ด้วยหลักสูตร micro-credential เมื่อเรียนจบจะมีใบรับรองและยืนยันว่าผู้เรียนผ่านเกณฑ์ระยะสั้น 8-12 ชั่วโมง สำหรับ Cyber-Avionics ที่เป็นศาสตร์และแนวปฏิบัติด้านความมั่นคงไซเบอร์สำหรับระบบอิเล็กทรอนิกส์บนอากาศยาน เชื่อมต่อสู่ใบอนุญาตสายการบินหรือใบรับรองมาตรฐาน Part-IS เพื่อลดเวลาฝึก 2) ดึงคนข้ามโดเมน เช่น DevOps สายพลังงาน Operational Technology (OT) ที่ทำงานเกี่ยวกับระบบฮาร์ดแวร์–ซอฟต์แวร์ที่ใช้ควบคุม ตรวจวัด และทำงานจริงกับกระบวนการทางกายภาพ เข้ามารีสกิลเป็น Security Operations Center (SOC) ที่ทำหน้าที่เป็นหน่วยงานกลางที่เฝ้าระวัง ตรวจจับ วิเคราะห์ และตอบสนองเหตุภัยคุกคามไซเบอร์ตลอด 24 ชั่วโมง ของสนามบินภายใน 6 เดือน 3) ใช้ AI ทอนภาระงานซ้ำ ๆ เช่น ให้ระบบอัจฉริยะช่วยกรองเหตุการณ์ Tier-1 หรือสร้าง playbook ตั้งต้นให้นักวิเคราะห์ และ 4) รักษาคนเก่า ด้วยโครงสร้างเวรสลับ week-on/week-off และเส้นทางความก้าวหน้าที่เชื่อมสาย cyber กับ safety โดยตรง มาตรการเหล่านี้ไม่เพียงปิดช่องว่างแรงงาน แต่ยังสร้างระบบนิเวศที่บุคลากรใหม่เติบโตได้เร็วและบุคลากรเก่าไม่ถูกดึงออกโดยอุตสาหกรรมอื่น

ความมั่นคงไซเบอร์ของการบินแขวนอยู่กับ “คน” พอ ๆ กับเทคโนโลยี หากไม่รีบออกแบบสายพานผลิต-เติม-รักษาคน พร้อมปล่อย AI เข้ามารับภาระงานระดับพื้นฐาน ช่องโหว่ด้านบุคลากรในวันนี้อาจกลายเป็นช่องโหว่ด้านความปลอดภัยการบินทั้งระบบภายในเวลาไม่กี่ปี

สรุป

ในทศวรรษที่การบินก้าวสู่ยุคดิจิทัลเต็มรูปแบบ อากาศยาน กลไกควบคุมจราจร และท่าอากาศยานต่างเชื่อมโยงกันด้วยข้อมูลเรียลไทม์ตลอดเส้นทางการบิน ความก้าวหน้าด้านเทคโนโลยีป้องกันไซเบอร์ตั้งแต่ตัวรับสัญญาณ ที่ทนการรบกวน ไปจนถึงศูนย์ที่ใช้ AI วิเคราะห์เหตุการณ์แม้จะช่วยเสริมเกราะป้องกันได้มาก แต่ก็ไม่อาจรับประกันความปลอดภัยได้หากขาดการเชื่อมต่อยังไม่ลงตัว

แม้เทคโนโลยีการป้องกันจะก้าวหน้า ความท้าทายอยู่ที่การจับคู่มาตรการไซเบอร์กับผลกระทบด้านความปลอดภัย จับคู่คนกับทักษะที่ต้องใช้ และจับคู่ข้อกำหนดระหว่างประเทศให้เป็นภาพเดียวกัน ทุกอย่างจะสำเร็จได้ ต้องมีแรงจูงใจร่วมระหว่างสายการบิน ท่าอากาศยาน และผู้ให้บริการเดินอากาศ ความมั่นคงและปลอดภัยไซเบอร์ของการบินไม่ใช่เรื่อง “เสริม” แต่คือ รากฐานของระบบการบินอัจฉริยะ หากเชื่อม “ห่วงโซ่ข้อมูล” ตลอดอากาศยาน-ท่าอากาศยาน-ศูนย์ควบคุมเข้ากับกรอบวิเคราะห์ความเสี่ยงที่มองเห็นความปลอดภัยไปด้วยกัน แล้วลงมือเสริมมาตรการเชิงเทคนิค กระบวนการ และบุคลากรอย่างสมดุล อุตสาหกรรมก็จะพร้อมรับมือภัยไซเบอร์ที่เปลี่ยนหน้าเร็วพอ ๆ กับเทคโนโลยีการบินที่กำลังทะยานขึ้นสู่ยุคน่านฟ้าดิจิทัลที่ออกแบบมาให้อากาศยานไร้คนขับ (U-space) และอากาศยานไฟฟ้า (eVTOL)

ข้อเสนอแนะ

ในขณะที่การบินเชื่อมโยงด้วยข้อมูลเรียลไทม์ตั้งแต่ขั้นเทกออฟจนถึงส่งกระเป๋าออกสายพานความมั่นคงไซเบอร์ จึงมิใช่ภารกิจเสริม หากเป็นสิ่งสำคัญควบคู่ความปลอดภัยการบิน (safety) ที่ต้องทำดังนี้

1. ผสานไซเบอร์เข้ากับความปลอดภัยอย่างเป็นระบบเริ่มต้นด้วยการนำข้อมูล Information-Security Management System (ISMS) ให้เข้ากับ Safety Management System (SMS) ให้เป็นวงจรเดียว วัดทั้งภัยไซเบอร์และผลกระทบด้านความปลอดภัย เพื่อตัดสินใจเชิงความเสี่ยงได้ทันที

2. ประเมินความเสี่ยงบนฐานข้อมูลจริงทั้งในท่าอากาศยาน และช่องโหว่แพตช์ซอฟต์แวร์อากาศยาน

3. เปิดหลักสูตร micro-credential 8-12 ชั่วโมง ต่อยอดสู่ใบรับรองเฉพาะทาง ลดเวลาอบรมจากปีเป็นสัปดาห์

4. สร้างวัฒนธรรมแบ่งปันเหตุการณ์แบบทันเวลา กำหนด data-sharing MOU ระหว่างสายการบิน สนามบิน ผู้ให้บริการเดินอากาศ ให้ข้อมูลเหตุไซเบอร์ที่อาจกระทบความปลอดภัยกระจายถึงทุกฝ่าย

บรรณานุกรม

CAE. (2025). ***CAE Aviation Talent Forecast*** (Online). Available: file:///C:/Users/user/Downloads/2025_CAE_Aviation_Talent_Forecast.pdf [2025, June 19].

EUROCONTROL. (2025). ***Cybersecurity – making aviation more resilient*** (Online). Available: https://www.eurocontrol.int/cybersecurity [2025, May 2].

European Commission. (2023). ***Commission Implementing Regulation (EU) 2023/203 of 27 October 2022*** (Online). Available: https://eur-lex.europa.eu/legal-ontent/EN/TXT/PDF/?uri=CELEX:32023R0203 [2025, July 2].

Federal Aviation Administration. (2020, August 14). ***FAA cybersecurity strategy (PL 115-254 Section 509)***. (Online). Available: https://www.faa.gov/sites/faa.gov/files/FAA_Cybersecurity_Strategy_PL_115-254_Sec509.pdf [2025, May 20].

GCAA. (2024). ***The UAE Civil Aviation Cybersecurity Policy*** (Online). Available: https://www.gcaa.gov.ae/en/epublication/Shared%20Documents/UAE%20CIVIL%20AVIATION%20CYBERSECURITY%20POLICY%20Issue%201.pdf?utm_source=chatgpt.com [2025, September 4].

Huntley, R. (2024, October 18). ***GNSS jamming and spoofing are a daily occurrence*** (Online). Available: https://www.eetimes.eu/gnss-jamming-and-spoofing-are-a-daily-occurrence/ [2025, May 29].

International Air Transport Association. (2024, February 15). ***Aviation value chain: An analysis of investor returns in 2022 within the aviation value chain*** (Online). Available: https://www.iata.org/en/iata-repository/publications/economic-reports/aviation-value-chain/ [2025, September 4].

International Air Transport Association. (2024). ***IATA Annual Safety Report – 2024 Executive Summary and Safety Overview*** (Online). Available: https://www.iata.org/contentassets/a8e49941e8824a058fee3f5ae0c005d9/safety-report-executive-summary-and-safety-overview-2024_final.pdf [2025, July 21].

International Civil Aviation Organization. (2025). ***Doc 10213-Unrestricted Global cyber risk considerations*** (1st ed advance unedited) (Online). Available: https://www.icao.int/aviationcybersecurity/Documents/Doc%2010213%20%28Unedited%29%20-%20Global%20Cyber%20Risk%20Considerations.EN.pdf [2025, April 28].

ISC2. (2024, October 31). ***2024 ISC2 Cybersecurity Workforce Study*** (Online). Available: https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study [2025, June 11].

Lind, N., Saxon, S., Vik, K., & Bouwer, J. (2024, November 1). ***Aviation value chain: Strong recovery brings profitability into view*** (Online). Available: https://www.mckinsey.com/industries/travel/our-insights/aviation-value-chain-strong-recovery-brings-profitability-into-view [2025, September 4].

Plucinska, J., Insinna, V., & Pearson, J. (2024, January 25). ***Aviation sector seeks urgent solutions for GPS interference*** (Online). Available: https://www.reuters.com/business/aerospace-defense/aviation-sector-seeks-urgent-solutions-gps-interference-2024-01-24/ [2025, June12].