# ปัจจัยเชิงสาเหตุที่มีอิทธิพลต่อขีดความสามารถความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพสำหรับกองทัพอากาศ

**ประยูร ธรรมาธิวัฒน์[1,*], ประสงค์ ปราณีตพลกรัง[2], พายัพ ศิรินาม[3]**
**[1,2,3]หลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีป้องกันประเทศ**
**สำนักบัณฑิตศึกษา โรงเรียนนายเรืออากาศนวมินทกษัตริยาธิราช**

*Received: 19 November 2024*
*Revised: 14 February 2025*
*Accepted: 14 February 2025*

## บทคัดย่อ

กองทัพอากาศมีภารกิจในการเตรียมกำลังและใช้กำลังทางอากาศเพื่อรักษาไว้ซึ่งความมั่นคงของประเทศ อย่างไรก็ตาม การรักษาความมั่นคงจะต้องดำเนินการทั้งทางกายภาพและดิจิทัล โดยเฉพาะทางดิจิทัลนั้นจะเน้นในโครงสร้างพื้นฐานทางดิจิทัลที่สำคัญยิ่งยวด ในขณะเดียวกันยังต้องคำนึงถึงความเสี่ยงและภัยคุกคามทางไซเบอร์อีกด้วย งานวิจัยนี้ มีวัตถุประสงค์เพื่อศึกษาและวิเคราะห์ปัจจัยเชิงสาเหตุที่มีอิทธิพลต่อขีดความสามารถความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพสำหรับกองทัพอากาศ ทั้งนี้ ผู้วิจัยใช้การวิเคราะห์สมการเชิงโครงสร้าง จากกลุ่มตัวอย่างจำนวน 810 คน ที่เป็นบุคลากรที่ปฏิบัติงานด้านเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ ผลการวิจัย พบว่า กองทัพอากาศมีความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับมากที่สุด และปัจจัยขีดความสามารถความพร้อมด้านบุคลากร กระบวนการ และเทคโนโลยีมีอิทธิพลเชิงบวกต่อความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ ดังนั้น การพัฒนาขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศจึงควรพัฒนาในด้านบุคลากร กระบวนการ และเทคโนโลยี ไปพร้อม ๆ กัน โดยเฉพาะอย่างยิ่ง ด้านบุคลากรและกระบวนการนั้นสำคัญมาก ที่จะช่วยเสริมสร้างความแข็งแกร่งในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศได้อย่างยั่งยืน นอกจากนี้ ผู้วิจัยได้นำเสนอกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อเสริมสร้างความพร้อมและเพิ่มประสิทธิภาพในการป้องกันภัยคุกคามทางไซเบอร์ของกองทัพอากาศ

**คำสำคัญ**: ความพร้อมทางไซเบอร์ ภัยคุกคามทางไซเบอร์ ขีดความสามารถทางไซเบอร์

[*]ผู้ประสานงานหลัก; อีเมล: pmgoth@gmail.com

# Causal Factors Influence the Cybersecurity Readiness Capability in the Royal Thai Air Force

**Prayoon Thammathiwat[1,*], Prasong Praneetpolgrang[2], Payap Sirinam[3]**
**[1,2,3]Master of Engineering Program in Defense Technology, Office of Graduate Studies, Navaminda Kasatriyadhiraj Royal Thai Air Force Academy, Saraburi, Thailand**

*Received: 19 November 2024*
*Revised: 14 February 2025*
*Accepted: 14 February 2025*

## Abstract

Royal Thai Air Force's mission is to prepare and deploy air power to maintain national security. However, maintaining security must be conducted both physically and digitally. In particular, the digital aspect focuses on critical digital infrastructure. At the same time, cyber risks and threats must also be taken into consideration. This research aims to study and analyze the causal factors that influence the cybersecurity readiness capability in the Royal Thai Air Force. The researchers employ structural equation modeling, using a sample of 810 personnel working in digital technology and cybersecurity for the Royal Thai Air Force. The research findings indicate that the Royal Thai Air Force has the highest level of readiness for cybersecurity. Additionally, the factors of personnel, processes, and technology readiness capability positively influence the cybersecurity readiness capability in the Royal Thai Air Force. Therefore, developing cybersecurity capabilities for the Royal Thai Air Force should focus on personnel, processes, and technology simultaneously. Particularly, the aspects of personnel and processes are of great importance, as it will significantly enhance the sustainable strength of the Royal Thai Air Force's cybersecurity. Additionally, we have proposed a cybersecurity framework aimed at enhancing the readiness and strengthening the effectiveness of the Royal Thai Air Force in preventing cyber threats.

**Keywords**: Cyber Readiness, Cyber Threats, Cyber Capabilities

[*]Corresponding Author; E-mail: pmgoth@gmail.com

## ความเป็นมาและความสำคัญของปัญหา

กองทัพอากาศมีภารกิจสำคัญในการรักษาความมั่นคงและเตรียมความพร้อมในการปกป้องราชอาณาจักร รวมถึงการพัฒนาประเทศและแก้ปัญหาความขัดแย้งต่าง ๆ ซึ่งภารกิจดังกล่าวเป็นไปได้ทั้งแบบการรบและไม่ใช่การรบ รวมถึงการช่วยเหลือด้านมนุษยธรรมและบรรเทาภัยพิบัติต่าง ๆ โดยยุทธศาสตร์กองทัพอากาศ 20 ปี (พ.ศ. 2561–2580) (ฉบับปรับปรุง พ.ศ. 2563) (Royal Thai Air Force, 2020) ให้ความสำคัญในการกำหนดยุทธศาสตร์เพื่อเสริมสร้างสมรรถนะและความพร้อมในการป้องกันประเทศและรักษาผลประโยชน์แห่งชาติ ซึ่งกองทัพอากาศจำเป็นต้องเตรียมกองกำลังให้มีความพร้อมสำหรับการปฏิบัติจริงมากที่สุด โดยหนึ่งในกลยุทธ์ที่กองทัพอากาศมุ่งเน้นคือการพัฒนาและประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสารในการเสริมสร้างขีดความสามารถด้านการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง ซึ่งกองทัพจำเป็นต้องพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร มีการประยุกต์ใช้เทคโนโลยีสมัยใหม่เข้ากับระบบสารสนเทศของกองทัพ และพัฒนาระบบสารสนเทศและระบบฐานข้อมูลที่มีประสิทธิภาพ

การพัฒนาด้านเทคโนโลยีสารสนเทศและการสื่อสารของกองทัพอากาศมีความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เพิ่มมากขึ้น เนื่องจากการเชื่อมโยงเครือข่ายข้อมูลที่สำคัญและการใช้เทคโนโลยีใหม่ ๆ ในการปฏิบัติการต่าง ๆ รวมถึงการพัฒนาของภัยคุกคามทางไซเบอร์ที่มีการโจมตีที่ซับซ้อนและที่รุนแรงมากขึ้น ทำให้ระบบการรักษาความมั่นคงปลอดภัยไซเบอร์แบบดั้งเดิมไม่เพียงพอต่อการจัดการกับภัยคุกคามทางไซเบอร์ที่ทันสมัย ดังนั้น การใช้เทคโนโลยีที่ทันสมัยเพื่อรับมือภัยคุกคามทางไซเบอร์ที่ซับซ้อนได้จึงเป็นแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กองทัพอากาศจำเป็นต้องดำเนินการ (Laohhapaibon and Kongwut, 2024) กอปรกับ การใช้เทคโนโลยีที่ทันสมัยมีความท้าทายในด้านต่าง ๆ เช่น ความพร้อมด้านบุคลากรที่มีความรู้และทักษะในการใช้เทคโนโลยี ความพร้อมด้านโครงสร้างพื้นฐานและกระบวนการดำเนินงานที่สอดคล้องกัน และความพร้อมด้านเทคโนโลยีที่มีความเข้ากันได้เพื่อให้การปฏิบัติงานสามารถดำเนินไปได้อย่างราบรื่น เป็นต้น

การวิจัยครั้งนี้ จึงมุ่งศึกษาปัจจัยเชิงสาเหตุที่มีอิทธิพลต่อขีดความสามารถความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพสำหรับกองทัพอากาศ ทั้งนี้ เพื่อพัฒนาแนวทางในการส่งเสริมและพัฒนาขีดความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ ในประเด็นด้านบุคลากร กระบวนการ และเทคโนโลยี นอกจากนี้ ผู้วิจัยพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับกองทัพอากาศ เพื่อเสริมสร้างความพร้อมและเพิ่มประสิทธิภาพในการป้องกันภัยคุกคามทางไซเบอร์ ซึ่งผลจากการวิจัยนี้จะช่วยให้สามารถระบุปัจจัยสำคัญและช่องโหว่ของการพัฒนาขีดความสามารถความพร้อมดังกล่าวให้กองทัพอากาศสามารถนำไปใช้เป็นแนวทางในการกำหนดนโยบายและกลยุทธ์เพื่อพัฒนาขีดความสามารถความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ

## วัตถุประสงค์ของการวิจัย

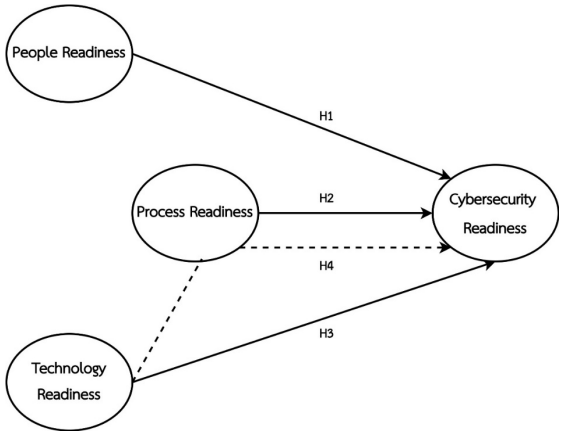
1. เพื่อศึกษาปัจจัยเชิงสาเหตุที่มีอิทธิพลต่อขีดความสามารถความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพสำหรับกองทัพอากาศ

2. เพื่อวิเคราะห์ปัจจัยเชิงสาเหตุที่มีอิทธิพลต่อขีดความสามารถความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพสำหรับกองทัพอากาศ

3. เพื่อนำเสนอกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับกองทัพอากาศ

## กรอบแนวคิดในการวิจัย

ผู้วิจัยพัฒนากรอบแนวคิดการวิจัยของปัจจัยเชิงสาเหตุที่มีอิทธิพลต่อขีดความสามารถความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพสำหรับกองทัพอากาศ (RTAF Cybersecurity Readiness) ประกอบด้วยความพร้อมด้านบุคลากร (People Readiness) ความพร้อมด้านกระบวนการ (Process Readiness) และความพร้อมด้านเทคโนโลยี (Technology Readiness) ดังแสดงในภาพที่ 1




**ภาพที่ 1** กรอบแนวคิดในการวิจัย

## สมมุติฐานการวิจัย

H1: ความพร้อมด้านบุคลากรมีอิทธิพลเชิงบวกต่อความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ

H2: ความพร้อมด้านกระบวนการมีอิทธิพลเชิงบวกต่อความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ

H3: ความพร้อมด้านเทคโนโลยีมีอิทธิพลเชิงบวกต่อความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ

H4: ความพร้อมด้านเทคโนโลยีมีอิทธิพลทางอ้อมต่อความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศผ่านความพร้อมด้านกระบวนการ

## เอกสารและงานวิจัยที่เกี่ยวข้อง

**คน กระบวนการ และเทคโนโลยี**

การพัฒนาขีดความสามารถความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศจำเป็นต้องพึ่งพาปัจจัยภายในองค์กรเพื่อพัฒนาขีดความสามารถดังกล่าว ผู้วิจัยทบทวนวรรณกรรมบนพื้นฐานของ Leavitt’s Diamond Framework (Leavitt, 1965) ที่กล่าวถึง 4 องค์ประกอบหลักขององค์กร ได้แก่ 1) บุคลากร (People) มุ่งเน้นที่ความรู้ ความสามารถและพฤติกรรมต่าง ๆ ของบุคลากรในองค์กร 2) งาน (Tasks) กระบวนการและกิจกรรมที่ดำเนินการเพื่อให้บรรลุเป้าหมายในการทำงาน 3) โครงสร้าง (Structure) การจัดองค์กรเพื่อแบ่งฝ่ายงาน

ความสัมพันธ์ และลำดับชั้นการบริหาร และ 4) เทคโนโลยี (Technology) เครื่องมือหรือเทคนิคที่ใช้เพื่อสนับสนุนการทำงาน ซึ่งความเปลี่ยนแปลงในแต่ละองค์ประกอบจะส่งผลกระทบต่อองค์ประกอบอื่น ๆ ทำให้เกิดการเปลี่ยนแปลงภายในองค์กรด้วย

Berlilana et al. (2021) ชี้ให้เห็นว่าเทคโนโลยีที่ทันสมัยและเพียงพอ การพัฒนาบุคลากรให้มีความรู้และทักษะ และการสร้างสภาพแวดล้อมให้อยู่ในบรรยากาศของการรักษาความมั่นคงปลอดภัยไซเบอร์จะส่งผลต่อการพัฒนาความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร ในขณะที่ Eilts (2020) พบว่า การให้ความสำคัญจากผู้บริหาร การปรับกิจกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับเป้าหมายขององค์กรและการปฏิบัติงานและการใช้เทคโนโลยีที่ไม่ซับซ้อนจนเกินไป ส่งผลที่ดีต่อการรักษาความมั่งคงปลอดภัยไซเบอร์ นอกจากนี้ Borgman, Mubarak, and Choo (2015) ศึกษาความพร้อมในการรักษาความมั่นคงปลอดภัย ไซเบอร์ของหน่วยงานรัฐบาลในประเทศออสเตรเลีย ได้กล่าวถึงความสำคัญของการสนับสนุนจากผู้บริหารและการสร้างความตระหนักรู้ให้แก่บุคลากร การใช้กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์และกลไกการกำกับดูแล รวมถึงการลงทุนในโครงสร้างพื้นฐานทางเทคโนโลยีและการควบคุมการเข้าถึงข้อมูลและระบบสำคัญขององค์กร โดยบ่งชี้ว่าการดำเนินงานต่าง ๆ อาจต้องเผชิญความท้าทายจากการขาดความพร้อมขององค์กรในด้านความรู้และทักษะของบุคลากร การดำเนินงานที่ไม่มีประสิทธิภาพ และการขาดแคลนงบประมาณ

**การพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับกองทัพอากาศ**

NIST Cybersecurity Framework version 1.1 คือ กรอบการทำงานที่พัฒนาโดย National Institute of Standards and Technology (NIST) เพื่อช่วยองค์กรจัดการและลดความเสี่ยงทางไซเบอร์อย่างมีประสิทธิภาพ (NIST, 2018) โดยกรอบมุ่งเน้นไปที่การดำเนินการที่สามารถปรับใช้ได้ในวงกว้างเพื่อสร้างความปลอดภัยให้กับข้อมูลและโครงสร้างพื้นฐานสำคัญ ประกอบด้วยห้าฟังก์ชันหลัก ได้แก่ การระบุ (Identify) การป้องกัน (Protect) การตรวจหา (Detect) การรับมือ (Respond) และการกู้คืน (Recover) ซึ่งครอบคลุมกระบวนการจัดการความปลอดภัยไซเบอร์ในทุกมิติ ทั้งยังเชื่อมโยงกับมาตรฐานสากล เช่น ISO/IEC 27001 เพื่อให้เหมาะสมกับองค์กรที่มีข้อจำกัดและความต้องการที่หลากหลาย การใช้งานกรอบนี้จะช่วยเพิ่มความสามารถในการรับมือภัยคุกคาม และส่งเสริมความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพได้ในระยะยาว

ISO/IEC 27001:2022 เป็นมาตรฐานสากลสำหรับการจัดการความมั่นคงปลอดภัยของสารสนเทศในองค์กร (International Organization for Standardization, 2022) โดยปรับปรุงจากเวอร์ชันก่อนหน้าเพื่อตอบสนองภัยคุกคามทางไซเบอร์ที่ซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว มาตรฐานนี้มุ่งเน้นการประเมินความเสี่ยง (Risk Assessment) และการกำหนดมาตรการควบคุม (Controls) เพื่อป้องกันและลดผลกระทบจากภัยคุกคามจากภายในและภายนอกองค์กร ผ่านระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศที่ครอบคลุมทั้งด้านเทคนิค การบริหารและกระบวนการดำเนินงาน นอกจากนี้ ยังเน้นการปรับปรุงอย่างต่อเนื่องเพื่อให้ระบบตอบสนองต่อความเสี่ยงที่มีการเปลี่ยนแปลงอยู่เสมอ

Enterprise Security Architecture (ESA) คือกรอบการทำงานเชิงกลยุทธ์ที่ออกแบบมาเพื่อช่วยองค์กรป้องกันและจัดการความเสี่ยงทางไซเบอร์อย่างเป็นระบบ (Sherwood, Clark, and Lynas, 2005) โดย ESA เป็นส่วนหนึ่งของ Enterprise Architecture (EA) ที่เน้นการผสานเป้าหมายทางธุรกิจเข้ากับมาตรการด้านความมั่นคงปลอดภัย ซึ่ง ESA ช่วยองค์กรระบุ วิเคราะห์ และตอบสนองต่อภัยคุกคามและช่องโหว่ในโครงสร้างของระบบเทคโนโลยีสารสนเทศ

อย่างมีประสิทธิภาพได้จากการกำหนดนโยบาย มาตรฐาน และแนวปฏิบัติที่ครอบคลุมทุกระดับ ตั้งแต่ระดับกลยุทธ์ถึงปฏิบัติการ นอกจากนี้ ESA ยังเน้นการบูรณาการมาตรการด้านความปลอดภัยเข้ากับกระบวนการทำงาน เพื่อป้องกันและลดผลกระทบจากภัยคุกคามทั้งในระยะสั้นและระยะยาว พร้อมช่วยให้องค์กรพัฒนาระบบที่ยืดหยุ่นและตอบสนองต่อการเปลี่ยนแปลงได้อย่างรวดเร็วในสภาพแวดล้อมที่ซับซ้อนและเสี่ยงภัยเพิ่มขึ้น

## วิธีดำเนินการวิจัย

**แบบแผนการวิจัย**

การวิจัยนี้เป็นการวิจัยเชิงปริมาณ (Quantitative Research) โดยทำการวิเคราะห์ปัจจัยที่เกี่ยวข้องกับตัวแปร และวิธีการทางสถิติในการช่วยวิเคราะห์ผล

**ประชากรและตัวอย่าง**

ประชากรที่ศึกษาในการวิจัย ได้แก่ บุคลากรที่ปฏิบัติหน้าที่ในหน่วยงานด้านเทคโนโลยีสารสนเทศ เทคโนโลยีดิจิทัล และความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ โดยข้อมูล ณ พ.ศ. 2567 มีจำนวนทั้งสิ้น 1,844 คน ผู้วิจัยได้กำหนดตัวอย่าง โดยใช้เกณฑ์สำหรับการเลือกตัวอย่างในการวิเคราะห์โมเดลสมการเชิงโครงสร้าง (Structural Equation Model: SEM) เท่ากับ 20 เท่า ของจำนวนพารามิเตอร์ (Hair, 2014) โดยจำนวนพารามิเตอร์ในโมเดลมี 18 พารามิเตอร์ ทำให้ได้ขนาดของประชากรกลุ่มตัวอย่างเท่ากับ 360 คน และเพื่อป้องกันแบบสอบถามที่ไม่สมบูรณ์ ผู้วิจัยจึงได้แจกแบบสอบถามรวมทั้งสิ้น 1,844 ฉบับ และได้รับผลการตอบแบบสอบถาม 810 ฉบับ

**เครื่องมือวิจัย**

ผู้วิจัยใช้แบบสอบถาม เรื่อง ความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับกองทัพอากาศ โดยแบบสอบถามแบ่งออกเป็น 3 ส่วน ได้แก่ ส่วนที่ 1 ข้อมูลส่วนบุคคลหรือหน่วยงานของผู้ตอบแบบสอบถาม ส่วนที่ 2 ข้อคำถามเกี่ยวกับความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับกองทัพอากาศ โดยใช้มาตรวัดของลิเคิร์ท 5 ระดับ (Five-point Likert Scale) และส่วนที่ 3 ความคิดเห็นหรือข้อเสนอแนะเพิ่มเติมในประเด็นด้านความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์

การศึกษาวิจัยนี้ตรวจสอบคุณภาพของแบบสอบถามด้วยการหาค่าความเที่ยงตรง (Validity) โดยส่งแบบสอบถามให้ผู้เชี่ยวชาญที่มีความรู้ความเข้าใจเฉพาะด้านจำนวน 5 ท่าน ตามเทคนิค Item Objective Congruence (IOC) โดยข้อคำถามมีค่า IOC มากกว่า 0.6 ทุกข้อ จากนั้นนำแบบสอบถามมาทดสอบความเชื่อมั่น (Reliability) โดยทดลองใช้ (Try Out) กับกลุ่มที่มีลักษณะคล้ายคลึงกับกลุ่มตัวอย่าง จำนวน 30 คน เพื่อตรวจสอบสัมประสิทธิ์แอลฟาของครอนบาก (Cronbach’s alpha Coefficient) ซึ่งผลการวิเคราะห์ความเชื่อมั่นของแบบสอบถาม พบว่ามีค่าสัมประสิทธิ์แอลฟาของครอนบาก อยู่ระหว่าง .831 - .933 จึงแสดงได้ว่าเครื่องมือแบบสอบถามมีความน่าเชื่อถือ (Nunnally, 1978)

**การวิเคราะห์ข้อมูล**

การวิเคราะห์ข้อมูลด้วยสถิติพรรณนา ได้แก่ ค่าเฉลี่ย (Mean) ค่าเบี่ยงเบนมาตรฐาน (Standard Deviation) และการวิเคราะห์โมเดลสมการโครงสร้าง (Structural Equation Model: SEM)

## ผลการวิจัย

ผลการศึกษาปัจจัยเชิงสาเหตุที่มีอิทธิพลต่อขีดความสามารถความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพสำหรับกองทัพอากาศ สามารถสรุปได้ว่ากองทัพอากาศมีความพร้อมด้านบุคลากร ($\overline{X}$ = 4.33, S.D. = 0.72) ความพร้อมด้านกระบวนการ ($\overline{X}$ = 4.40, S.D. = 0.66) ความพร้อมด้านเทคโนโลยี ($\overline{X}$ = 4.23, S.D. = 0.77) และความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ ($\overline{X}$ = 4.27, S.D. = 0.75) อยู่ในระดับมากที่สุด ดังแสดงตารางที่ 1

**ตารางที่ 1** ระดับปัจจัยที่มีผลกระทบต่อความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับกองทัพอากาศ

| ปัจจัย | $\overline{X}$ | S.D. | แปลผล |
|---|---|---|---|
| 1. ความพร้อมด้านบุคลากร | 4.33 | .643 | มากที่สุด |
| 2. ความพร้อมด้านกระบวนการ | 4.41 | .579 | มากที่สุด |
| 3. ความพร้อมด้านเทคโนโลยี | 4.22 | .682 | มากที่สุด |
| 4. ความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ | 4.27 | .654 | มากที่สุด |

ผลการวิเคราะห์ความเหมาะสมของตัวแปร เพื่อตรวจสอบความความสัมพันธ์ระหว่างตัวแปรก่อนนำไปวิเคราะห์สมการเชิงโครงสร้าง พบว่า ตัวแปรทั้ง 4 ตัวแปรมีค่าสหสัมพันธ์ระหว่างตัวแปร จำนวน 6 คู่ มีค่าอยู่ระหว่าง .690 – 0.795 แสดงให้เห็นว่าตัวแปรมีความสัมพันธ์กันในระดับไม่สูงเกินไป จึงไม่มีปัญหาสหสัมพันธ์ร่วมเชิงพหุ (Multicollinearity) และตัวแปรทั้งหมดอยู่ในองค์ประกอบร่วมกัน เมื่อพิจารณาค่าสถิติ Barlett’s Test of Sphericity มีค่าเท่ากับ 2560, df = 6, $p < .001$ และเมทริกซ์สัมประสิทธิ์สหสัมพันธ์ไม่เป็นเมทริกซ์เอกลักษณ์ (Identity Matrix) อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.001 ดังนั้น ตัวแปรจึงมีความสัมพันธ์กันอย่างเพียงพอที่จะสามารถนำไปวิเคราะห์องค์ประกอบได้ สอดคล้องกับผลการวิเคราะห์ Kaiser-Mayer-Olkin (KMO) เท่ากับ 0.851 จึงสามารถสรุปได้ว่าตัวแปรมีความเหมาะสมที่จะนำไปวิเคราะห์สมการเชิงโครงสร้าง

ผลการวิเคราะห์ความตรงเชิงโครงสร้างของตัวแปร (Construct Validity) ประกอบด้วยการวัดความตรงเชิงสอดคล้อง (Convergent Validity) และความตรงเชิงจำแนก (Discriminant validity) ดังนี้

การวัดความตรงเชิงสอดคล้อง (Convergent Validity) เพื่อวัดว่าตัวแปรสังเกตได้สามารถเป็นตัวชี้วัดของตัวแปรแฝงได้หรือไม่ โดยพิจารณาจากค่าความเชื่อมั่นรวมของตัวแปรแฝง (Composite Reliability: CR) ที่แสดงถึงระดับที่ตัวแปรสังเกตได้ร่วมกันอธิบายตัวแปรแฝง ค่าเฉลี่ยความแปรปรวนที่สกัดได้ (Average Variance Extract: AVE) ที่แสดงถึงความแปรปรวนของตัวแปรแฝงที่ถูกอธิบายได้จากตัวแปรสังเกตได้ และความเชื่อมั่น (Cronbach's Alpha) ที่แสดงถึงค่าความเที่ยงหรือความเชื่อมั่นของแบบสอบถาม โดยผลจากการวิเคราะห์พบว่า ตัวแปรแฝงทุกตัวแปรมีค่า CR มากกว่า 0.7 ตัวแปรแฝงทุกตัวแปรมีค่า AVE มากกว่า 0.5 แสดงว่าตัวแปรสังเกตได้ร่วมกันอธิบายตัวแปรแฝงได้ในระดับที่ยอมรับได้ (Fornell and Larcker, 1981) และตัวแปรแฝงทุกตัวแปรมีค่าความเชื่อมั่นมากกว่า 0.7 (Nunnally, 1978) ดังนั้น จึงสามารถกล่าวได้ว่าทุกตัวแปรมีความตรงเชิงสอดคล้อง ดังแสดงในตารางที่ 2

**ตารางที่ 2** การวัดความตรงเชิงสอดคล้อง

| ตัวแปร | Factor Loading | CR | AVE | Cronbach |
|---|---|---|---|---|
| **People Readiness** | | 0.867 | 0.685 | 0.866 |
| Awareness | .77 | | | |
| Training and Learning | .85 | | | |
| Research and Development | .86 | | | |
| **Process Readiness** | | 0.920 | 0.697 | 0.925 |
| Strategy and Plan | .86 | | | |
| Cybersecurity Evaluation | .86 | | | |
| Cybersecurity Framework | .85 | | | |
| Cybersecurity Coordination | .77 | | | |
| Cybersecurity Improvement | .83 | | | |
| **Technology Readiness** | | 0.934 | 0.740 | 0.936 |
| Quality and Quantity | .85 | | | |
| Modern and Efficient | .84 | | | |
| Protecting Devices | .87 | | | |
| Detect and Response | .89 | | | |
| Access and Control | .85 | | | |
| **Cybersecurity Readiness** | | 0.846 | 0.648 | 0.843 |
| Cybersecurity Awareness | .76 | | | |
| Policy | .87 | | | |
| Cybersecurity Infrastructure | .78 | | | |

ผลการความตรงเชิงจำแนก (Discriminant Validity) ซึ่งเป็นการวัดว่าตัวแปรแฝงแต่ละตัวแปรมีความแตกต่างกันหรือไม่ โดยพิจารณาจากค่ารากที่สองของ AVE ที่ควรมีมากกว่าค่าสหสัมพันธ์ระหว่างตัวแปร (Hair, 2014; Fornell and Larcker, 1981) พบว่า ตัวแปรแฝงทั้ง 4 ตัวแปร มีค่ารากที่สองของ AVE มากกว่าค่าสหสัมพันธ์ระหว่างตัวแปร แสดงว่าโมเดลมีการจำแนกตัวแปรได้อย่างเหมาะสม ดังแสดงในตารางที่ 3

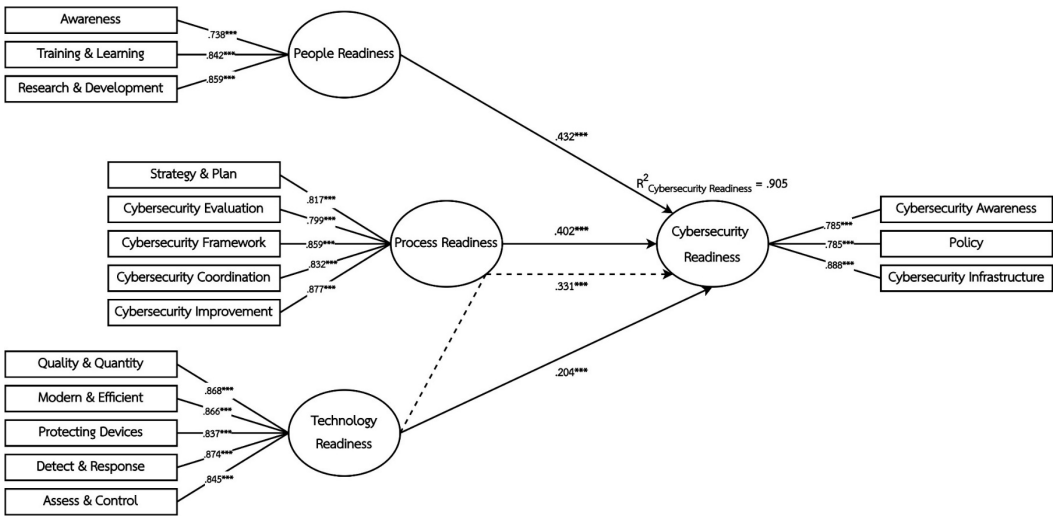
**ตารางที่ 3** การวัดความตรงเชิงจำแนก

| | People | Process | Technology | CS Readiness |
|---|---|---|---|---|
| People | *0.828* | | | |
| Process | .772 | *0.835* | | |
| Technology | .690 | .745 | *0.860* | |
| CS Readiness | .764 | .795 | .793 | *0.805* |

หมายเหตุ: ตัวเอียงในเส้นทแยงมุม คือ ค่ารากที่สองของ AVE

ผลการวิเคราะห์โมเดลการวัด (Measurement Model) เพื่อวัดความสัมพันธ์ระหว่างตัวแปรสังเกตได้และตัวแปรแฝง โดยใช้การวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmatory Factor Analysis: CFA) พบว่าในการวิเคราะห์ตัวแปรสังเกตได้ทั้งหมดมีค่าน้ำหนักอยู่ระหว่าง 0.76 – 0.89 ดังแสดงในตารางที่ 3 ซึ่งมากกว่าเกณฑ์ที่กำหนด คือ 0.7 (Hair, 2014) แสดงว่า ตัวแปรสังเกตได้สามารถอธิบายตัวแปรแฝงได้เป็นอย่างเหมาะสม

ผลการวิเคราะห์โมเดลเชิงโครงสร้าง ผลการทดสอบความสอดคล้องของโมเดลเชิงโครงสร้างของปัจจัยเชิงสาเหตุที่มีอิทธิพลต่อขีดความสามารถความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพสำหรับกองทัพอากาศ ตามสมมติฐานกับข้อมูลเชิงประจักษ์ ซึ่งจากการพิจารณาค่าดัชนีความสอดคล้องในครั้งแรกพบว่า โมเดลตามสมมุติฐานยังไม่สอดคล้องข้อมูลเชิงประจักษ์ จึงทำการปรับโมเดลโดยพิจารณาจากค่าดัชนีในการปรับ (Modification Indices) จนกระทั่งดัชนีความสอดคล้องผ่านเกณฑ์ที่กำหนด ดังนี้ $\chi^2$/df = 3.967, *p*-value = .000, GFI = .952, NFI = .972, TLI = .969, CFI = .979, RMSEA = .061, และ RMR = .021 แสดงให้เห็นว่า โมเดลที่พัฒนาขึ้นมีความสอดคล้องกับข้อมูลเชิงประจักษ์ ดังแสดงในภาพที่ 2 ทั้งนี้ ผลการวิเคราะห์พบว่า 1) ความพร้อมด้านบุคลากร มีอิทธิพลทางตรงเชิงบวกต่อความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ โดยมีขนาดอิทธิพลเท่ากับ .432 ที่ระดับนัยสำคัญ .001 2) ความพร้อมด้านกระบวนการ มีอิทธิพลทางตรงเชิงบวกต่อความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ โดยมีขนาดอิทธิพลเท่ากับ .402 ที่ระดับนัยสำคัญ .001 3) ความพร้อมด้านเทคโนโลยี มีอิทธิพลทางตรงเชิงบวกต่อความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ โดยมีขนาดอิทธิพลเท่ากับ .204 ที่ระดับนัยสำคัญ .001 4) ความพร้อมด้านเทคโนโลยีมีอิทธิพลทางอ้อมต่อความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศผ่านความพร้อมด้านกระบวนการ โดยมีขนาดอิทธิพลเท่ากับ .331 ที่ระดับนัยสำคัญ .001 และ 5) ความพร้อมด้านบุคลากร กระบวนการ และเทคโนโลยี สามารถร่วมกันอธิบายความแปรปรวนของความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ ได้ร้อยละ 90.5




หมายเหตุ : *** = p < .001

**ภาพที่ 2** ผลการวิเคราะห์โมเดลเชิงโครงสร้าง

ในงานวิจัยนี้ ผู้วิจัยได้พัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับกองทัพอากาศ บนพื้นฐานของการศึกษาและวิเคราะห์ปัจจัยเชิงสาเหตุที่มีอิทธิพลต่อขีดความสามารถความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพสำหรับกองทัพอากาศ ประกอบกับ การทบทวนวรรณกรรมที่เกี่ยวข้อง อาทิ NIST Cybersecurity Framework version 1.1, ISO/IEC 27001:2022 และ Enterprise Security Architecture (ESA) ในที่สุดจะได้กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับกองทัพอากาศ ดังแสดงในภาพที่ 3


**ภาพที่ 3** กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับกองทัพอากาศ

กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับกองทัพอากาศดังนำเสนอในภาพที่ 3 นั้นจะประกอบด้วย 8 องค์ประกอบหลักที่ครอบคลุมตั้งแต่การการบริหารองค์กร การดำเนินงาน และการให้ความสนับสนุนการดำเนินงานจากองค์กร โดยมีรายละเอียดดังนี้

1. นโยบายและการกำกับดูแล (Policy and Governance) เป็นส่วนสำคัญที่กองทัพอากาศต้องให้ความสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อส่งเสริมกระบวนการดำเนินงานและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยมีองค์ประกอบดังนี้

1.1 นโยบาย (Policy) การกำหนดนโยบายที่ชัดเจน เพื่อให้ทุกหน่วยงานได้เห็นถึงหลักการและทิศทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งครอบคลุมถึงการจัดการความเสี่ยงทางไซเบอร์ ขั้นตอนการดำเนินงาน การให้สิทธิ์บุคลากร การพัฒนาของบุคลากร และการสร้างวัฒนธรรมที่ดีทางไซเบอร์

1.2 การกำกับดูแล (Governance) การสร้างโครงสร้างองค์กรที่ส่งเสริมมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สามารถดำเนินการได้อย่างมีประสิทธาพ ครอบคลุมถึงการกำหนดบทบาทและความรับผิดชอบของผู้บริหารและบุคลากร การจัดตั้งคณะกรรมการและคณะทำงาน และการประเมินผลเพื่อปรับปรุงนโยบายและกระบวนทำงานอย่างต่อเนื่อง

1.3 ข้อกำหนด (Regulation) การดำเนินการตามข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเคร่งครัด ทั้งในระดับองค์กร ประเทศ และนานาชาติ เพื่อให้สามารถภารกิจและกิจกรรมได้อย่างต่อเนื่อง และลดความเสี่ยงจากการถูกกีดกันหรือลงโทษ

2. การสนับสนุนจากองค์กร (Organizational Support) เป็นรากฐานสำคัญที่ช่วยให้การดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศประสบความสำเร็จ โดยกองทัพอากาศต้องให้ความสนับสนุนใน 3 ด้าน ได้แก่ เงินทุน ทรัพยากร และบุคลากร

2.1 การสนับสนุนด้านเงินทุน (Financial Support) ต้องเพียงพอต่อการพัฒนาระบบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างยั่งยืน โดยลงทุนในเทคโนโลยีและเครื่องมือที่ทันสมัยและมีประสิทธิภาพ การฝึกอบรมบุคลากร และเงินทุนสำหรับการตอบสนองและฟื้นฟูหลังเกิดเหตุการณ์โจมตีทางไซเบอร์

2.2 ทรัพยากร (Resource) ต้องมีโครงสร้างพื้นฐานด้านดิจิทัล เทคโนโลยีและเครื่องมือที่เพียงพอทันสมัยและมีประสิทธิภาพ การจัดหาอุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์ การใช้ศูนย์ข้อมูล ข่าวกรองภัยคุกคามทางไซเบอร์ และการพัฒนาระบบการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการใช้ระบบสำรองข้อมูล

2.3 บุคลากร (Human Resource) โดยการส่งเสริมให้บุคลากรมีความเชี่ยวชาญหรือมีความรู้พื้นฐานด้วยการฝึกอบรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่บุคลากรทุกระดับ การแต่งตั้งทีมผู้เชี่ยวชาญหรือจ้างผู้เชี่ยวชาญจากภายนอกเพื่อรับมือกับเหตุการณ์โจมตีทางไซเบอร์

3. การระบุทรัพย์สินและความเสี่ยง (Asset and Risk Management) เป็นกระบวนการสำคัญที่ช่วยให้องค์กรสามารถปกป้องทรัพยากรที่สำคัญและลดความเสี่ยงที่อาจเกิดจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ การจัดการในส่วนนี้ประกอบด้วย การจัดทำรายการทรัพย์สิน การประเมินความเสี่ยง และการจัดลำดับความสำคัญ

3.1 การจัดทำรายการสินทรัพย์ (Asset Inventory) เพื่อการระบุทรัพย์สินที่องค์กรครอบครองเป็นขั้นตอนแรกที่ช่วยให้เข้าใจว่าอะไรคือสิ่งที่ต้องปกป้อง รวมถึงฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และระบบเครือข่าย โดยการจัดทำบัญชีสินทรัพย์และอัปเดตอย่างสม่ำเสมอ

3.2 การประเมินความเสี่ยง (Risk Assessment) เพื่อระบุความเสี่ยงที่เกี่ยวข้องกับทรัพย์สินที่สำคัญและประเมินผลกระทบที่อาจเกิดขึ้น โดยการวิเคราะห์ว่าอะไรคือภัยคุกคามที่อาจเกิดขึ้น เช่น การโจมตีทางไซเบอร์ มัลแวร์ หรือการสูญเสียข้อมูล การประเมินผลกระทบถึงความรุนแรงที่อาจเกิดขึ้นหากทรัพย์สินถูกโจมตีหรือสูญเสีย และการคำนวณความเสี่ยง

3.3 การจัดลำดับความสำคัญ (Prioritization) เพื่อให้องค์กรสามารถจัดสรรทรัพยากรและความพยายามไปที่การปกป้องทรัพย์สินที่มีมูลค่าสูงและความสำคัญต่อภารกิจมากที่สุด ซึ่งอาจจัดลำดับความสำคัญของสินทรัพย์ตามมูลค่าทางธุรกิจ ความสำคัญต่อภารกิจ และความอ่อนไหวของข้อมูล

4. การป้องกัน (Protection) เป็นหัวใจสำคัญในการลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อระบบและข้อมูลของกองทัพอากาศ โดยมีการดำเนินการใน 3 องค์ประกอบ ได้แก่ การควบคุมการเข้าถึง การบริหารจัดการระบบ และการสร้างความตระหนักรู้

4.1 การควบคุมการเข้าถึง (Access Control) โดยกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบตามบทบาทและหน้าที่ ใช้การยืนยันตัวตนหลายปัจจัยเพื่อเพิ่มความปลอดภัย การจำกัดการเข้าถึงห้องศูนย์ข้อมูลหรืออุปกรณ์สำคัญเฉพาะบุคลากรที่ได้รับอนุญาต และใช้ระบบบันทึกกิจกรรม (Audit Logs) เพื่อติดตามและวิเคราะห์พฤติกรรมที่ผิดปกติ

4.2 การบริหารจัดการระบบ (System Management) เพื่อเพิ่มความปลอดภัยของการดำเนินงานโดยการติดตั้งแพตช์ความปลอดภัย (Security Patches) และการอัปเดตซอฟต์แวร์อย่างสม่ำเสมอ ติดตั้งโปรแกรม

ป้องกันมัลแวร์และไฟร์วอลล์ที่ทันสมัย พร้อมทั้งอัปเดตฐานข้อมูลไวรัสอย่างต่อเนื่อง และระบบตรวจจับการบุกรุก และใช้การเข้ารหัสข้อมูลสำหรับการรับส่งข้อมูลที่สำคัญ

4.3 การสร้างความตระหนักรู้ (Awareness Creation) ให้แก่บุคลากร โดยจัดอบรมบุคลากรเกี่ยวกับวิธีการป้องกันภัยคุกคาม เช่น การหลีกเลี่ยงฟิชชิง (Phishing) และวิธีจัดการข้อมูลอย่างปลอดภัย การฝึกซ้อมสถานการณ์จำลองการโจมตีไซเบอร์ การแจ้งเตือนภัยคุกคามใหม่ ๆ ผ่านระบบอีเมลหรือประกาศ และการสร้างความตระหนักรู้ในระดับองค์กรเพื่อให้บุคลากรเข้าใจและปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างจริงจัง

5. การตรวจหา (Detection) เป็นขั้นตอนสำคัญในกระบวนการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มุ่งเน้นการระบุภัยคุกคามหรือเหตุการณ์ผิดปกติที่อาจเกิดขึ้นในระบบและเครือข่ายขององค์กร เพื่อให้สามารถตอบสนองและแก้ไขปัญหาได้อย่างรวดเร็ว ประกอบด้วย 3 องค์ประกอบ ได้แก่ ระบบตรวจสอบภัยคุกคาม การวิเคราะห์ข้อมูล และการแจ้งเตือน

5.1 ระบบเฝ้าสังเกตภัยคุกคาม (Threat Monitoring Systems) โดยใช้ระบบตรวจจับการบุกรุกเพื่อเฝ้าระวังและตรวจจับกิจกรรมที่ผิดปกติในเครือข่าย ระบบป้องกันการบุกรุกเพื่อเพิ่มความสามารถในการตอบสนองโดยการหยุดกิจกรรมที่เป็นอันตราย และระบบบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Information and Event Management) เพื่อวิเคราะห์และตรวจจับความผิดปกติแบบเรียลไทม์

5.2 การวิเคราะห์ข้อมูล (Data Analysis) โดยการรวบรวมและวิเคราะห์ข้อมูลกิจกรรมเข้าออก จากเซิร์ฟเวอร์ และอุปกรณ์เครือข่าย เพื่อค้นหาความผิดปกติ การใช้เทคโนโลยีการเรียนรู้ของเครื่อง และการเรียน รู้เชิงลึกในการวิเคราะห์ข้อมูลเพื่อระบุรูปแบบที่บ่งชี้ถึงภัยคุกคามและทำนายความเสี่ยงล่วงหน้า และการวิเคราะห์ข่าวกรองภัยคุกคามทางไซเบอร์ ฐานข้อมูลมัลแวร์หรือรายงานภัยคุกคาม เพื่อช่วยระบุภัยที่มีแนวโน้มจะเกิดขึ้น

5.3 การแจ้งเตือน (Alerting) โดยใช้ระบบแจ้งเตือนอัตโนมัติที่สามารถแจ้งเตือนทันทีเมื่อระบบตรวจพบเหตุการณ์ผิดปกติ เช่น การพยายามเข้าถึงโดยไม่ได้รับอนุญาต หรือการโจมตี DDoS และแบ่งลำดับความสำคัญของเหตุการณ์เพื่อให้ทีมงานตอบสนองต่อภัยคุกคามที่สำคัญที่สุดก่อน รวมทั้งการแจ้งเตือนหลากหลายช่องทาง และบันทึกรายงานเหตุการณ์ที่ตรวจพบเพื่อใช้ในการวิเคราะห์และปรับปรุงระบบในอนาคต

6. การตอบสนอง (Response) เป็นขั้นตอนสำคัญที่ช่วยให้องค์กรสามารถจัดการกับภัยคุกคามไซเบอร์หรือเหตุการณ์ผิดปกติที่เกิดขึ้นได้อย่างมีประสิทธิภาพ เพื่อลดความเสียหายและนำไปสู่การฟื้นฟูระบบให้กลับสู่ภาวะปกติโดยเร็วที่สุด โดยมี 3 องค์ประกอบ ได้แก่ แผนตอบสนองเหตุการณ์ ทีมรับมือภัยคุกคาม และการสื่อสาร

6.1 แผนตอบสนองเหตุการณ์ (Incident Response Plan) โดยระบุขั้นตอนและกระบวนการที่ชัดเจนในการจัดการภัยคุกคามหรือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยต้องมีขั้นตอนต่อไปนี้ การเตรียมความพร้อมในการจัดหาเครื่องมือและทรัพยากรที่จำเป็น การระบุเหตุการณ์เพื่อวิเคราะห์และตรวจสอบ การควบคุมและจำกัดผลกระทบ การขจัดภัยคุกคาม การกู้คืนระบบ และการทวทวนเพื่อปรับปรุง

6.2 ทีมรับมือภัยคุกคาม (Cybersecurity Incident Response Team) มีหน้าที่รับผิดชอบในการตอบสนองและจัดการเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ที่ประกอบด้วยผู้เชี่ยวชาญในด้านต่าง ๆ ได้แก่ หัวหน้าทีมทำหน้าที่ตัดสินใจและควบคุมการดำเนินงาน ผู้เชี่ยวชาญด้านเทคนิค ผู้เชี่ยวชาญด้านกฎหมาย และผู้ประสานงาน ซึ่งบุคลากรในทีมจำเป็นต้องได้รับการพัฒนาอย่างสม่ำเสมอ

6.3 การสื่อสาร (Communication) เพื่อสร้างความเข้าใจแก่ผู้เกี่ยวข้อง โดยการแจ้งให้ผู้บริหารและบุคลากรที่เกี่ยวข้องทราบถึงเหตุการณ์ที่เกิดขึ้น รวมถึงความคืบหน้าในการจัดการ ประสานงานกับหน่วยงานกำกับดูแล และผู้ให้บริการเทคโนโลยี ในกรณีข้อมูลรั่วไหล ต้องแจ้งผู้ที่ได้รับผลกระทบตามข้อกำหนดทางกฎหมาย และเตรียมข้อความที่เหมาะสมสำหรับแถลงต่อสื่อและสาธารณชน เพื่อรักษาความเชื่อมั่นในองค์กร

7. การฟื้นฟู (Recovery) เป็นขั้นตอนสำคัญที่มุ่งเน้นการคืนสภาพการทำงานของระบบและข้อมูลให้กลับสู่ภาวะปกติหลังจากเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบหรือโครงสร้างพื้นฐานขององค์กร โดยมี 3 องค์ประกอบ ได้แก่ แผนกู้คืนระบบ การสำรองข้อมูล และการประเมินผลหลังเหตุการณ์

7.1 แผนกู้คืนระบบ (Disaster Recovery Plan) เป็นแผนที่กำหนดขั้นตอนและกระบวนการในการฟื้นฟูระบบที่ได้รับผลกระทบให้กลับมาทำงานได้อย่างรวดเร็วและมีประสิทธิภาพ โดยระบุระบบที่สำคัญที่จำเป็นต้องกู้คืนก่อน ดำเนินกระบวนการกู้คืน กำหนดกรอบเวลาที่ระบบต้องกลับมาทำงานได้ การทดสอบแผน อย่างสม่ำเสมอเพื่อให้มั่นใจว่าแผนสามารถปฏิบัติได้จริง

7.2 การสำรองข้อมูล (Backup) เพื่อให้มั่นใจว่าองค์กรสามารถกู้คืนข้อมูลที่สูญหายหรือเสียหายได้อย่างรวดเร็ว โดยดำเนินการสำรองข้อมูลและทดสอบกระบวนการกู้คืนข้อมูลอย่างสม่ำเสมอเพื่อให้มั่นใจว่าข้อมูลสำรองสามารถนำกลับมาใช้ได้จริง

7.3 การประเมินผลหลังเหตุการณ์ (Post-Incident Evaluation) เพื่อให้องค์กรเรียนรู้จากเหตุการณ์และปรับปรุงกระบวนการเพื่อป้องกันเหตุการณ์ในอนาคต โดยการวิเคราะห์เหตุการณ์เพื่อระบุสาเหตุและผลกระทบ รวบรวมบทเรียนในสิ่งที่ทำได้ดีและสิ่งที่ต้องปรับปรุง และจัดทำรายงานเพื่อนำมาใช้ในการปรับปรุงพัฒนาแผนการฟื้นฟู

8. การปรับปรุง (Improvement) เป็นกระบวนการที่ช่วยให้องค์กรสามารถพัฒนาระบบความมั่นคงปลอดภัยไซเบอร์ให้มีประสิทธิภาพสูงขึ้นอย่างต่อเนื่อง โดยมุ่งเน้นการเรียนรู้จากเหตุการณ์ที่ผ่านมาเพื่อรองรับภัยคุกคามที่เปลี่ยนแปลงอยู่เสมอ การปรับปรุงนี้ประกอบด้วย การปรับปรุงและแก้ไขปัญหา และการตรวจสอบระบบเป็นระยะ

8.1 ดำเนินการแก้ไขและปรับปรุง (Corrective Actions and Improvements) เพื่อลดความเสี่ยงและเพิ่มประสิทธิภาพของระบบ อ้างอิงจากบทเรียนและปัญหาที่เกิดขึ้น โดยวิเคราะห์สาเหตุของปัญหา กำหนดแนวทางแก้ไข และติดตามผลการแก้ไข รวมถึงการสื่อสารเพื่อแจ้งให้บุคลากรที่เกี่ยวข้องทราบถึงการปรับปรุงและแนวทางใหม่ที่กำหนดขึ้น

8.2 การตรวจสอบระบบเป็นระยะ (Periodic System Reviews) เพื่อให้องค์กรสามารถระบุช่องโหว่และปัญหาที่อาจเกิดขึ้นได้ก่อนที่จะกลายเป็นภัยคุกคาม อาจทำโดยตรวจสอบโครงสร้างพื้นฐาน เช่น การตั้งค่าเครือข่าย ไฟร์วอลล์ และการอัปเดตซอฟต์แวร์ การทดสอบเจาะระบบ ตรวจสอบบันทึก (Logs) เพื่อระบุพฤติกรรมที่ผิดปกติ และจัดทำตารางการตรวจสอบ เช่น รายเดือน รายไตรมาส หรือเมื่อมีการเปลี่ยนแปลงระบบ

ทั้งนี้ กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับกองทัพอากาศที่ผู้วิจัยได้พัฒนาขึ้นนี้ ได้ทำการประเมินในประเด็น ความเหมาะสม การยอมรับ และประสิทธิภาพ จากผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จำนวน 8 คน ประกอบด้วย ผู้เชี่ยวชาญจากกองทัพอากาศ ภาคเอกชน หน่วยงานรัฐวิสาหกิจ และมหาวิทยาลัย ซึ่งผลการประเมินแสดงให้เห็นว่ากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับกองทัพอากาศที่พัฒนาขึ้นมีความเหมาะสมอยู่ในระดับมาก มีการยอมรับอยู่ในระดับมากที่สุด และมีประสิทธิภาพอยู่ในระดับมาก ดังแสดงในตารางที่ 4

**ตารางที่ 4** ผลการประเมินกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับกองทัพอากาศ

| ข้อคำถาม | ระดับการประเมิน | |
|---|---|---|
| 1. กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับกองทัพอากาศ **มีความเหมาะสม** อยู่ในระดับใด | 4.13 | มาก |
| 2. กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับกองทัพอากาศ **มีการยอมรับ** อยู่ในระดับใด | 4.25 | มากที่สุด |
| 3. กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับกองทัพอากาศ **มีประสิทธิภาพ** อยู่ในระดับใด | 4.13 | มาก |
| **รวม** | **4.16** | **มาก** |

## อภิปรายผล

ความพร้อมด้านบุคลากร กระบวนการ และเทคโนโลยี มีอิทธิพลเชิงบวกต่อขีดความสามารถความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ แสดงให้เห็นว่า กองทัพอากาศจำเป็นต้องพัฒนาความพร้อมทั้ง 3 ด้านให้มีประสิทธิภาพร่วมกัน โดยความพร้อมด้านบุคลากรมีอิทธิพลมากที่สุด รองลงมาคือความพร้อมด้านกระบวนการ และความพร้อมด้านเทคโนโลยี ตามลำดับ

การสร้างความตระหนักรู้และการฝึกอบรมให้แก่บุคลากร เป็นสิ่งจำเป็นที่กองทัพอากาศต้องทำเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ แต่การกระทำดังกล่าวอาจยังไม่เพียงพอให้บุคลากรมีพฤติกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้ Bada et al. (2015) รายงานว่ากลยุทธ์การสร้างความตระหนักรู้และการฝึกอบรมที่จะนำไปสู่พฤติกรรมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคคล ได้แก่ 1) การจัดเนื้อหาการฝึกอบรมที่เข้าถึงง่ายสอดคล้องกับพฤติกรรมการปฏิบัติงานของผู้คน เพื่อให้ผู้คนยอมรับและปรับพฤติกรรม 2) การจัดเนื้อหาการฝึกอมรมต้องพิจารณาตามความสอดคล้องกับวัฒนธรรมการทำงานที่แตกต่างกันในแต่ละหน่วยงาน นอกจากนั้น การสร้างความหวาดกลัวเกี่ยวกับภัยคุกคามทางไซเบอร์ให้แก่ผู้คนอาจได้ผล แต่จะส่งให้บุคคลมีความเครียดในการทำงานเพิ่มมากขึ้น

การเปลี่ยนผ่านรูปแบบการทำงานเข้าสู่การทำงานแบบดิจิทัลที่ทุกองค์การกำลังพัฒนาเพื่อสร้างคุณค่าที่เพิ่มขึ้นให้แก่การดำเนินงาน นำมาซึ่งความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เช่น การแลกเปลี่ยนข้อมูลสำคัญระหว่างหน่วยงานจำเป็นต้องมีมาตรการสำหรับการป้องกันการขโมยและการเข้าถึงข้อมูลดังกล่าว ดังนั้น กองทัพอากาศซึ่งเป็นหน่วยงานที่มีโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญต่อประเทศ จำเป็นต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ (Saeed et al., 2023b) เพื่อสร้างความมั่นใจว่ากระบวนการดำเนินงานในรูปแบบดิจิทัลของกองทัพอากาศปราศจากการคุกคามจากภัยคุกคามทางไซเบอร์และป้องกันการรั่วไหลของข้อมูลสำคัญ

เทคโนโลยีที่มีประสิทธิภาพและทันสมัย มีความจำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ สืบเนื่องจากกรณีความพร้อมด้านบุคลากรที่อาจยังไม่มีความตระหนักรู้ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การใช้เทคโนโลยีที่มีประสิทธิภาพและทันสมัยจึงเป็นแนวทางการบรรเทาความเสี่ยงที่ดี กองทัพอากาศอาจต้องลงทุนในด้าน

เทคโนโลยีการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น การเรียนรู้ของเครื่อง และปัญญาประดิษฐ์ ควบคู่ไปกับการฝึกอบรมบุคลากรให้สามารถใช้งานเครื่องมือดังกล่าวเพื่อลดข้อผิดพลาดที่เกิดจากมนุษย์ลงได้ (Annarelli et al., 2020)

นอกจากนี้ ผลการวิจัยชี้ให้เห็นว่าความพร้อมด้านเทคโนโลยีมีบทบาทสำคัญในการเสริมสร้างความพร้อมด้านกระบวนการให้มีความแข็งแกร่งยิ่งขึ้น อีกทั้ง เมื่อความพร้อมด้านกระบวนการได้รับการพัฒนาขึ้นจนมีประสิทธิภาพที่ดีจะส่งผลต่อความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศได้อย่างมีนัยสำคัญ อย่างไรก็ตาม ข้อมูลดังกล่าวสะท้อนให้เห็นถึงความจำเป็นในการลงทุนและพัฒนาเทคโนโลยีควบคู่กับการปรับปรุงกระบวนการเพื่อสร้างรากฐานที่มั่นคงต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ในระยะยาว ซึ่งสอดคล้องกับงานวิจัยของ Zhang et al. (2021) ที่ชี้ให้เห็นว่าการลงทุนในเทคโนโลยีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์นั้น จะช่วยลดความเสี่ยงเชิงระบบขององค์กร อีกทั้งยังสร้างความเชื่อมั่นให้กับผู้รับบริการว่าองค์กรมีความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ด้วย

การพัฒนาขีดความสามารถความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ เพื่อบรรเทาความเสี่ยงจากภัยคุกคามทางไซเบอร์ จำเป็นต้องพัฒนาความพร้อมใน 3 ด้านหลัก ได้แก่ ความพร้อมด้านบุคลากร กระบวนการ และเทคโนโลยี โดยเฉพาะอย่างยิ่งความพร้อมด้านบุคลากรที่ต้องสร้างความตระหนักรู้และทักษะด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ก้าวทันภัยคุกคามทางไซเบอร์ที่มีการพัฒนาและเปลี่ยนแปลงรูปแบบการโจมตีอย่างสม่ำเสมอ ซึ่งบุคลากรที่มีทักษะด้านการรรักษาความมั่นคงปลอดภัยไซเบอร์จะช่วยเพิ่มขีดความสามารถความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ (Hasan et al., 2021) การลงทุนในด้านเทคโนโลยีสมัยใหม่ เช่น การเรียนรู้ของเครื่องและปัญญาประดิษฐ์ ที่ต้องดำเนินไปควบคู่กับการฝึกอบรมบุคลากรให้มีทักษะในการใช้เทคโนโลยีขั้นสูง โดยกองทัพอากาศต้องบริหารจัดการเนื้อหาอบรมให้เหมาะสมกับพฤติกรรมการปฏิบัติงานที่แตกต่างกันของแต่ละหน่วยงาน เพื่อบุคลากรได้รับความรู้และทักษะในการใช้เทคโนโลยีที่ลงทุนไปสำหรับป้องกันภัยคุกคามทางไซเบอร์ได้อย่างเต็มที่ (Neri et al., 2024)

นอกจากนั้น การเปลี่ยนผ่านทางดิจิทัลได้เพิ่มความเสี่ยงทางไซเบอร์ให้กับกองทัพอากาศในกระบวนการทำงานซึ่งครอบคลุมในทุกมิติที่มีการใช้เทคโนโลยีดิจิทัล การใช้มาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เชื่อถือได้จึงเป็นสิ่งจำเป็นในการบรรเทาความเสี่ยงทางไซเบอร์ เช่น การใช้ระบบข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligent) เพื่อแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์ที่ทันต่อเหตุการณ์และเชื่อถือได้ให้หน่วยงานภายในนำไปใช้ และมีการแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอกอย่างสม่ำเสมอ รวมถึงมีการนำเสนอข้อมูลในรูปแบบที่ผู้คนเข้าใจได้ง่าย (Saeed et al., 2023a) จะช่วยเพิ่มขีดความสามารถความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศได้อย่างมีประสิทธิภาพ

อีกทั้ง กองทัพอากาศเป็นหน่วยงานภาครัฐที่มีความสำคัญยิ่งต่อประเทศ จึงตกเป็นเป้าหมายการโจมตีของผู้ร้ายทางไซเบอร์ที่ต้องการเข้าถึงข้อมูลสำคัญ ทดสอบความสามารถของตนเอง ทำลายชื่อเสียงของกองทัพเพื่อวัตถุประสงค์ใด ๆ ดังนั้น การพัฒนาขีดความสามารถความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ในด้านบุคลากร กระบวนการ และเทคโนโลยีอาจไม่เพียงพอต่อการหลีกเลี่ยงภัยคุกคามทางไซเบอร์ได้ กองทัพอากาศจำเป็นต้องพิจารณากลยุทธ์ในด้านอื่นด้วย เช่น การพัฒนากรอบการประเมินความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังงานวิจัยของ Cheang (2009) ที่เสนอกรอบการประเมินความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีจำนวน 46 ตัวชี้วัด ครอบคลุมใน 3 ด้าน ได้แก่ บุคลากร โครงสร้างพื้นฐาน และสภาพแวดล้อม

สำหรับประเมินความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานภาครัฐในประเทศกำลังพัฒนา เพื่อให้หน่วยงานทราบถึงจุดแข็งและจุดอ่อนของตนเอง ซึ่งจะช่วยให้กำหนดกลยุทธ์ในการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างครอบคลุม และ Georgiadou et al. (2021) เสนอกรอบการประเมินการรักษาความมั่นคงปลอดภัยไซเบอร์บนพื้นฐาน MITRE ATTandCK (Adversarial Tactics, Techniques, and Common Knowledge) ที่ครอบคลุมในด้านการดำเนินงานขององค์กรและบุคลากร โดยมุ่งเน้นไปที่การรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานที่สำคัญ ได้แก่ เทคโนโลยีดิจิทัล และเทคโนโลยีดำเนินงาน (Operational Technology)

อย่างไรก็ตาม เราจะพบว่า การพัฒนากรอบการประเมินความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่กล่าวมา แสดงให้เห็นว่านักวิจัยได้ให้ความสำคัญในด้านบุคลากรเป็นอย่างมาก ยิ่งไปกว่านั้น การกำหนดมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์อาจไม่สามารถบังคับให้บุคลากรปฏิบัติตามมาตรการได้ ทำให้ยังมีช่องโหว่จากความผิดพลาดของบุคลากร (Pollini et al., 2022) ดังนั้น การพัฒนาขีดความสามารถความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศจึงจำเป็นต้องมีมาตรการที่ครอบคลุม โดยเฉพาะอย่างยิ่งกลยุทธ์ในการพัฒนาความพร้อมด้านบุคลากรและกระบวนการ ซึ่งผู้วิจัยได้นำเสนอกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับกองทัพอากาศ เพื่อเสริมสร้างความแข็งแกร่งและความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุมกระบวนการทำงานและเพิ่มประสิทธิภาพให้สามารถดำเนินงานได้อย่างต่อเนื่องในกรณีที่เกิดเหตุการณ์โจมตีทางไซเบอร์

## ข้อเสนอแนะ

**1. ข้อเสนอแนะในการนำผลวิจัยไปใช้**

ผลการวิจัยฉบับนี้ พบว่า ปัจจัยด้านบุคลากรมีความสำคัญยิ่งต่อขีดความสามารถความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ ดังนั้น การพัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพอากาศ จึงควรให้ความสำคัญในการพัฒนาบุคลากรทั้งในด้านความตระหนักรู้และทักษะในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

**2. ข้อเสนอแนะในการวิจัยครั้งถัดไป**

การวิจัยในครั้งถัดไปควรพิจารณาปัจจัยอื่นที่ส่งผลต่อขีดความสามารถความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพสำหรับกองทัพอากาศ เช่น ผลกระทบจากวัฒนธรรมองค์กรในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และผลกระทบจากการใช้เทคโนโลยีขั้นสูง ได้แก่ การเรียนรู้ของเครื่องและปัญญาประดิษฐ์ในการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นต้น

## เอกสารอ้างอิง

Royal Thai Air Force. (2020). *Royal Thai Air Force Strategy for 20 years (2018 - 2037) (Revised edition 2020).* [Online]. Retrieved from: https://welcome-page.rtaf.mi.th/blog/e-ksaarephyaephr-11/yuththsaastrk-ngthaph-aakaas-20-pii-ph-s-2561-2580-38. (in Thai)

Laohhapaibon, P., and Kongwut, O. (2024). Integrating Artificial Intelligence (AI) and Artificial General Intelligence (AGI) to Enhance the Cybersecurity System of the Royal Thai Air Force's Cyber Center. *NKRAFA Journal of Science and Technology*, *20*(1), 131-140.

Annarelli, A., Nonino, F., and Palombi, G. (2020). Understanding the management of cyber resilient systems. *Computers and Industrial Engineering, 149*, 106829. https://doi.org/10.1016/j.cie.2020.106829

Bada, M., Sasse, A. M., and Nurse, J. R. C. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? Presented at the *International Conference on Cyber Security for Sustainable Society (CSSS)*.

Berlilana, Noparumpa, T., Ruangkanjanases, A., Hariguna, T., and Sarmini. (2021). Organization benefit as an outcome of organizational security adoption: The role of cyber security readiness and technology readiness. *Sustainability*, *13*(24), 13761. https://doi.org/10.3390/su132413761

Borgman, B., Mubarak, S., and Choo, K. K. R. (2015). Cyber security readiness in the South Australian Government. *Computer Standards and Interfaces, 37*, 1-8. https://doi.org/10.1016/j.csi.2014.06.002

Cheang, S. (2009). Conceptual model for cybersecurity readiness assessment for public institutions in developing country: Cambodia. *The Proceedings of the 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology,* 1411-1418. https://doi.org/10.1109/ICCIT.2009.242

Eilts, D. (2020). *An Empirical Assessment of Cybersecurity Readiness and An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses Resilience in Small Businesses*. [Online]. Retrieved from: https://nsuworks.nova.edu/gscis_etd

Fornell, C., and Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50. https://doi.org/10.2307/3151312

Georgiadou, A., Mouzakitis, S., and Askounis, D. (2021). Assessing MITRE ATTandCK risk using a cyber-security culture framework. *Sensors, 21*(9), 3267. https://doi.org/10.3390/s21093267

Hair, J. F., Anderson, R. E., and Black, W. C. (2014). *Multivariate data analysis*. 7th ed. Upper Saddle River, NJ: Prentice Hall.

Hasan, S., Ali, M., Kurnia, S., and Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications, 58*, 102726. https://doi.org/10.1016/j.jisa.2020.102726

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements.* International Organization for Standardization. [Online]. Retrieved from: https://www.iso.org/standard/82875.html

Leavitt, H. J. (1965). Applied organisational change in industry: Structural, technological and humanistic approaches. In J. G. March (Ed.), *Handbook of organisation.* Rand McNally and Company. Chicago, Illinois.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S.: Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

Neri, M., Niccolini, F., and Martino, L. (2024). Organizational cybersecurity readiness in the ICT sector: A quanti-qualitative assessment. *Information and Computer Security, 32*(1), 38-52. https://doi.org/10.1108/ICS-05-2023-0084

Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). New York: McGraw-Hill.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., and Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology and Work, 24*(3), 371-390. https://doi.org/10.1007/s10111-021-00683-y

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., and Alabbad, D. A. (2023b). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors, 23*(15), 6666. https://doi.org/10.3390/s23156666

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., and Almuhaideb, A. M. (2023a). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors, 23*(16), 7273. https://doi.org/10.3390/s23167273

Sherwood, J., Clark, A., and Lynas, D. (2005). *Enterprise security architecture: A business-driven approach*. CRC Press.

Zhang, Y., Zhang, C., and Xu, Y. (2021). Effect of data privacy and security investment on the value of big data firms. *Decision Support Systems*, *146*. https://doi.org/10.1016/j.dss.2021.113543