



การวิเคราะห์ปัจจัยการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล

นางสาวผ่องศรี ประสมบุญ

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต

สาขาวิชาระบบสารสนเทศเพื่อการจัดการ

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ปีการศึกษา 2568

ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

การวิเคราะห์ปัจจัยการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล



นางสาวผ่องศรี ประสมบุญ

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร

วิทยาศาสตรมหาบัณฑิต

สาขาวิชาระบบสารสนเทศเพื่อการจัดการ

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ปีการศึกษา 2568

ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ



ใบรับรองการค้นคว้าอิสระ

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง การวิเคราะห์ปัจจัยการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล

โดย นางสาวผ่องศรี ประสมบุญ

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาระบบสารสนเทศเพื่อการจัดการ

คณบดีคณะเทคโนโลยีสารสนเทศและ
นวัตกรรมดิจิทัล

(ผู้ช่วยศาสตราจารย์ ดร.สุนันทา สดสี)

คณะกรรมการสอบการค้นคว้าอิสระ

ประธาน

(รองศาสตราจารย์ ดร.อลิสา ทรงศรีวิทยา)

อาจารย์ที่ปรึกษา

(ผู้ช่วยศาสตราจารย์ ดร.ศักดิ์ชาย ตั้งวรรณวิทย์)

กรรมการ

(รองศาสตราจารย์ ดร.มหศักดิ์ เกตุจำ)

ชื่อ : นางสาวผ่องศรี ประสมบุญ
 ชื่อการค้นคว้าอิสระ : การวิเคราะห์ปัจจัยการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล
 สาขาวิชา : ระบบสารสนเทศเพื่อการจัดการ
 มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
 อาจารย์ที่ปรึกษาการค้นคว้าอิสระ : ผู้ช่วยศาสตราจารย์ ดร.ศักดิ์ชาย ตั้งวรรณวิทย์
 ปีการศึกษา : 2568

บทคัดย่อ

การค้นคว้าอิสระเรื่อง การวิเคราะห์ปัจจัยการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล มีวัตถุประสงค์เพื่อศึกษาระดับการรับรู้ความพร้อมด้านความมั่นคงปลอดภัย และวิเคราะห์ปัจจัยที่มีอิทธิพลต่อการรับรู้ดังกล่าว การวิจัยใช้ระเบียบวิธีแบบผสมผสาน โดยเก็บข้อมูลเชิงปริมาณด้วยแบบสอบถามมาตราส่วน 5 ระดับ และวิเคราะห์ด้วยสถิติเชิงพรรณนา การวิเคราะห์องค์ประกอบ และการถดถอยเชิงเส้นพหุคูณ

ผลการวิจัยพบว่า ระดับการรับรู้ด้าน IT Security Readiness อยู่ในระดับมาก (Mean = 3.85) โดยเฉพาะความตระหนักรู้ด้านภัยคุกคามมีค่าเฉลี่ยสูงที่สุด (Mean = 4.12) ผลการทดสอบสมมติฐานพบว่า ความตระหนักรู้ด้านภัยคุกคาม (SA) และการสนับสนุนจากองค์กร (SP) มีอิทธิพลเชิงบวกต่อการรับรู้ประโยชน์ (PU) และความต้องการพัฒนาระบบ (Dev) อย่างมีนัยสำคัญทางสถิติ ขณะที่ SA มีอิทธิพลเชิงลบต่อความสามารถในการควบคุม (CT) แต่ การสนับสนุนจากองค์กร (SP) มี อิทธิพลเชิงบวกต่อความสามารถในการควบคุม (CT)

ข้อค้นพบชี้ให้เห็นว่า การยกระดับมาตรฐานความมั่นคงปลอดภัยให้สอดคล้องกับ International Organization for Standardization ISO/IEC 27001:2022 และ HAIT Plus ควร ดำเนินควบคู่ระหว่างการสร้างความตระหนักรู้และการสนับสนุนเชิงโครงสร้างจากองค์กร

(มีจำนวนทั้งสิ้น 71 หน้า)

คำสำคัญ : ความมั่นคงปลอดภัยทางไซเบอร์, HAIT Plus, ISO/IEC 27001:2022, การรับรู้, ผู้บริหารโรงพยาบาล

อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก

Name : Miss Pongsri Prasomboon
Independent Study Title : Factors Analysis of The Perception of Cybersecurity Standards for Hospitals
Major Field : Management Information Systems
King Mongkut's University of Technology North
Bangkok
Independent Study Advisor : Assistant Professor Dr. Sakchai Tangwannawit
Academic Year : 2025

ABSTRACT

This independent study, entitled “An Analysis of Perceptual Factors of Cybersecurity Standards for Hospitals,” aimed to (1) examine the level of perceived IT security readiness and (2) analyze the factors influencing such perceptions in the hospital context. A mixed-methods approach was employed. Quantitative data were collected using a five-point Likert scale questionnaire and analyzed through descriptive statistics, exploratory factor analysis (EFA), and multiple linear regression.

The findings revealed that the overall level of IT Security Readiness was at a high level (Mean = 3.85). Among the examined dimensions, Security Awareness (SA) showed the highest mean score (Mean = 4.12). Hypothesis testing indicated that Security Awareness (SA) and Organizational Support (SP) had significant positive effects on Perceived Usefulness (PU) and System Development Intention (Dev). However, SA demonstrated a significant negative effect on Controllability (CT), whereas SP had a significant positive effect on CT.

The results suggest that enhancing cybersecurity standards in alignment with International Organization for Standardization ISO/IEC 27001:2022 and HAIT Plus should involve not only raising security awareness but also strengthening organizational support mechanisms and structural governance to ensure sustainable cybersecurity development in hospitals.

(Total xx Pages)

Keywords: Cybersecurity, HAIT Plus, ISO/IEC 27001:2022, Perception, Hospital Executives

Advisor

กิตติกรรมประกาศ

การศึกษาค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงได้ด้วยความรู้ ความร่วมมือ และการสนับสนุนจากหลายฝ่าย ผู้วิจัยขอกราบขอบพระคุณเป็นอย่างสูงต่อบุคคลและหน่วยงานที่มีส่วนสำคัญดังต่อไปนี้

ขอกราบขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร.ศักดิ์ชาย ตั้งวรรณวิทย์ อาจารย์ที่ปรึกษาหลัก และประธานกรรมการที่ปรึกษาการค้นคว้าอิสระ ที่ได้ให้ความอนุเคราะห์เวลาอันมีค่าในการให้คำปรึกษา แนะนำแนวทางการศึกษา ตรวจแก้ไขข้อบกพร่อง ตลอดจนให้ข้อเสนอแนะทางวิชาการ ที่ทรงคุณค่าอย่างต่อเนื่อง ส่งผลให้งานวิจัยฉบับนี้มีความสมบูรณ์และเป็นไปตามมาตรฐานทางวิชาการ

ขอกราบขอบพระคุณ รองศาสตราจารย์ ดร.อลิสา ทรงศรีวิทยา ประธานสอบป้องกันการค้นคว้าอิสระ และ รองศาสตราจารย์ ดร.มหศักดิ์ เกตุฉำ กรรมการสอบการค้นคว้าอิสระ ที่ได้กรุณาให้ข้อคิดเห็น ข้อเสนอแนะ และแนวทางในการปรับปรุงแก้ไขงานวิจัยให้มีความชัดเจนและสมบูรณ์ยิ่งขึ้น

ขอขอบพระคุณ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ และคณะผู้บริหารของบัณฑิตวิทยาลัย ที่ได้มอบโอกาสทางการศึกษา สนับสนุนทรัพยากรทางวิชาการ ตลอดจนสิ่งอำนวยความสะดวกต่าง ๆ อันเอื้อต่อการดำเนินการวิจัยในครั้งนี้

ขอขอบคุณกลุ่มตัวอย่างและผู้ตอบแบบสอบถามทุกท่าน ที่ได้สละเวลาอันมีค่าในการให้ข้อมูลอันเป็นประโยชน์ ซึ่งนับเป็นองค์ประกอบสำคัญที่ทำให้งานวิจัยครั้งนี้สำเร็จลุล่วงตามวัตถุประสงค์

ขอขอบคุณเพื่อนร่วมงานและเพื่อนนักศึกษาทุกท่าน ที่ได้ให้คำแนะนำ แบ่งปันความรู้ และแลกเปลี่ยนประสบการณ์ทางวิชาการตลอดกระบวนการศึกษา

สุดท้ายนี้ ผู้วิจัยขอกราบขอบพระคุณครอบครัวที่ให้การสนับสนุนอย่างเต็มที่ ทั้งในด้านกำลังใจ ความเข้าใจ และความอดทนตลอดระยะเวลาการศึกษา ซึ่งเป็นแรงผลักดันสำคัญที่ทำให้ผู้วิจัยสามารถดำเนินการศึกษาค้นคว้าอิสระฉบับนี้จนสำเร็จลุล่วงด้วยดี

ผ่องศรี ประสมบูรณ์

สารบัญ

หน้า

บทคัดย่อภาษาไทย	ง
บทคัดย่อภาษาอังกฤษ	จ
กิตติกรรมประกาศ	ฉ
สารบัญ	ช
สารบัญตาราง	ณ
สารบัญรูปภาพ	ญ
บทที่ 1 บทนำ	1
1.1 ความเป็นมาและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์ของการวิจัย	4
1.3 สมมติฐานของการวิจัย	4
1.4 ขอบเขตของการวิจัย	4
1.5 ตัวแปรที่ศึกษา	5
1.6 นิยามศัพท์เฉพาะ	6
1.7 ประโยชน์ที่คาดว่าจะได้รับ	7
บทที่ 2 เอกสารและงานวิจัยที่เกี่ยวข้อง	8
2.1 มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์	8
2.2 มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล	13
2.3 ข้อกำหนด ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับ โรงพยาบาล	15
2.4 ทฤษฎีปัจจัยด้านการรับรู้และพฤติกรรมของบุคลากร	19
2.5 ทฤษฎีที่เกี่ยวข้องกับการยอมรับเทคโนโลยีสารสนเทศ	20
2.6 งานวิจัยที่เกี่ยวข้อง	21
บทที่ 3 วิธีดำเนินการวิจัย	23
3.1 กำหนดปัญหาและวัตถุประสงค์การวิจัย	23
3.2 ประชากรและกลุ่มตัวอย่าง	24
3.3 เครื่องมือที่ใช้ในการวิจัย	25
3.4 วิธีดำเนินการวิจัยและการเก็บรวบรวมข้อมูล	26
3.5 วิธีการวิเคราะห์ข้อมูล	27
บทที่ 4 ผลการวิจัย	28
4.1 ผลการวิเคราะห์ข้อมูลทั่วไป	28
4.2 ผลการวิเคราะห์ตัวแปรแต่ละด้าน	30
4.3 การวิเคราะห์องค์ประกอบเชิงสำรวจ	34
4.4 ผลการทดสอบสมมติฐานด้วยการวิเคราะห์การถดถอยเชิงเส้น	41

สารบัญ (ต่อ)

	หน้า
บทที่ 5 สรุปผล อภิปรายผล และข้อเสนอแนะ	54
5.1 สรุปผล	54
5.2 อภิปรายผล	57
5.3 ข้อเสนอแนะ	59
บรรณานุกรม	62
ภาคผนวก	65
ประวัติผู้เขียน	71



สารบัญตาราง

		หน้า
ตารางที่ 2-1	โครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุข	16
ตารางที่ 4-1	จำนวนและร้อยละของข้อมูลทั่วไปของผู้ตอบแบบสอบถาม	28
ตารางที่ 4-2	ค่าเฉลี่ยและค่าส่วนเบี่ยงเบนมาตรฐานปัจจัยด้านความพร้อมความมั่นคงเทคโนโลยีสารสนเทศ	31
ตารางที่ 4-3	ค่าเฉลี่ยและค่าส่วนเบี่ยงเบนมาตรฐานปัจจัยด้านบุคลากร	31
ตารางที่ 4-4	ค่าเฉลี่ยและค่าส่วนเบี่ยงเบนมาตรฐานปัจจัยด้านการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์	32
ตารางที่ 4-5	ค่าเฉลี่ยและค่าส่วนเบี่ยงเบนมาตรฐานปัจจัยด้านความพร้อมในการบริหารจัดการตามมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์	33
ตารางที่ 4-6	สรุปผล KMO และ Bartlett's Test of Sphericity ตามรอบการวิเคราะห์	34
ตารางที่ 4-7	สรุปช่วงค่า MSA รายตัวแปรและข้อสังเกตจำแนกตามรอบการวิเคราะห์	35
ตารางที่ 4-8	สรุปน้ำหนักองค์ประกอบและค่า Uniqueness จากการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ครั้งที่ 1	37
ตารางที่ 4-9	สรุปน้ำหนักองค์ประกอบและค่า Uniqueness จากการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ครั้งที่ 2	38
ตารางที่ 4-10	สรุปน้ำหนักองค์ประกอบและค่า Uniqueness จากการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ครั้งที่ 3	39
ตารางที่ 4-11	สรุปน้ำหนักองค์ประกอบและค่า Uniqueness จากการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ครั้งที่ 4	40
ตารางที่ 4-12	ผลการวิเคราะห์ถดถอยพหุคูณของตัวแปร ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (SA) และการสนับสนุนจากองค์กร (SP) ที่มีต่อการรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (PU)	43
ตารางที่ 4-13	ค่าสัมประสิทธิ์ถดถอยของตัวแปรอิสระ ของตัวแปรความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (SA) และการสนับสนุนจากองค์กร (SP) ที่มีต่อการรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (PU)	44
ตารางที่ 4-14	ผลการวิเคราะห์ถดถอยพหุคูณของตัวแปรความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (SA) และการสนับสนุนจากองค์กร (SP) ที่มีต่อความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (CT)	46
ตารางที่ 4-15	ค่าสัมประสิทธิ์ถดถอยของตัวแปรอิสระ ของตัวแปรความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (SA) และการสนับสนุนจากองค์กร (SP) ที่มีต่อความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (CT)	46

สารบัญตาราง (ต่อ)

หน้า

ตารางที่ 4-16	ผลการวิเคราะห์ถดถอยพหุคูณของตัวแปร ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (SA) และการสนับสนุนจากองค์กร (SP) ที่มีต่อความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Dev)	49
ตารางที่ 4-17	ค่าสัมประสิทธิ์ถดถอยของตัวแปรอิสระ ของตัวแปรความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (SA) และการสนับสนุนจากองค์กร (SP) ที่มีต่อความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Dev)	50
ตารางที่ 4-18	สรุปผลการทดสอบสมมติฐานโดยรวม	52



สารบัญรูปภาพ

หน้า

ภาพที่ 1-1 รายงานความเสี่ยงระดับโลกในระยะยาว (10 ปี) จำแนกตามกลุ่มผู้มีส่วนได้ส่วนเสีย	1
ภาพที่ 1-2 รายงานค่าเฉลี่ยการโจมตีทางไซเบอร์แต่ละอุตสาหกรรมทั่วโลกรายสัปดาห์	2
ภาพที่ 2-1 แสดงแนวคิดหลัก PDCA	10
ภาพที่ 2-2 กรอบ NIST Cybersecurity Framework 2.0	12



บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันภัยคุกคามทางไซเบอร์ถือเป็นภัยที่ก่อให้เกิดความเสียหายต่อตัวบุคคล หน่วยงาน ทั้งภาครัฐ ภาคเอกชน เช่น หน่วยงานความมั่นคง หน่วยงานพลังงาน รวมถึงหน่วยงานด้าน สาธารณสุข ในระดับประเทศ และระดับโลก

จากรายงานความเสี่ยงระดับโลก ปี ค.ศ. 2025 (The Global Risks Report 2025) ด้านความ เสี่ยงระดับโลกในระยะยาว 10 ปี โดยจำแนกตามกลุ่ม พบว่า ความเสี่ยงที่เกิดจากการใช้เทคโนโลยี สารสนเทศในหน่วยงานภาครัฐ (Government) คือ ข้อมูลสารสนเทศที่เป็นเท็จและบิดเบือน (Misinformation and disinformation) อยู่ในอันดับ 1 และการจารกรรมข้อมูลทางไซเบอร์และ สงครามทางไซเบอร์ (Cyber espionage and warfare) อยู่ในอันดับ 6

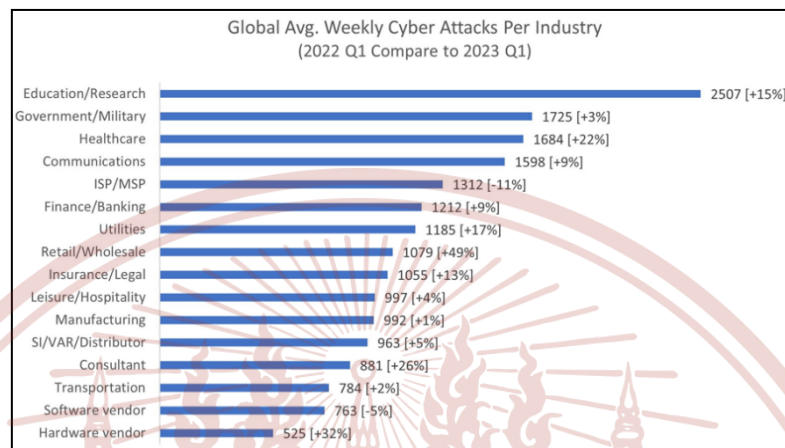


ภาพที่ 1-1 รายงานความเสี่ยงระดับโลกในระยะยาว (10 ปี) จำแนกตามกลุ่มผู้มีส่วนได้ส่วนเสีย

ที่มา: The Global Risk Report 2025. World Economic Forum

รายงานดังกล่าวยังพูดถึงความเสี่ยงระยะสั้น หรือ 2 ปี ความเสี่ยงที่เกิดจากการใช้งาน แพลตฟอร์มดิจิทัลที่เพิ่มขึ้นและปริมาณเนื้อหาที่สร้างโดยปัญญาประดิษฐ์ ที่เพิ่มมากขึ้นทำให้เกิด ข้อมูลที่ผิดพลาดและมีการบิดเบือนเนื้อหาจนเป็นข้อมูลที่เป็นเท็จ รวมถึงการเปลี่ยนแปลงสู่ระบบ ดิจิทัลมากขึ้นเป็นเหตุที่ทำให้บุกรุกไปยังหน่วยงานของภาครัฐได้ง่ายขึ้นเช่นกัน รายงานของ Journal of The American Medical Association ยังพบว่า การโจมตีทางไซเบอร์ต่อสถานพยาบาลและระบบ ให้บริการทางด้านสาธารณสุขมีค่าเฉลี่ยที่ 1,684 ครั้งต่อสัปดาห์ ในไตรมาสที่ 1 ของปี พ.ศ. 2566

เพิ่มขึ้นจากปี 2565 ถึง 22% (สืบค้นจาก <https://www.weforum.org/agenda/2023/05/cyber-attacks-on-healthcare-rise-zero-trust/>, 2567)



ภาพที่ 1-2 รายงานค่าเฉลี่ยการโจมตีทางไซเบอร์แต่ละอุตสาหกรรมทั่วโลกรายสัปดาห์

ที่มา: Global Cybersecurity Continue to Rise with Africa and APAC Suffering Most.

Checkpoint Research

จากสถิติภัยคุกคามทางไซเบอร์ในประเทศไทยในปี พ.ศ. 2568 โดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือ สกมช. พบว่า หน่วยงานด้านสาธารณสุขอยู่ในอันดับที่ 6 จากหน่วยงานที่ถูกโจมตีจากภัยคุกคามทางไซเบอร์ มีจำนวน 136 ครั้ง โดยมีสาเหตุจากบุคลากรมีความรู้เรื่องภัยคุกคามทางไซเบอร์เพียง 52.32% และมีการนำเทคโนโลยีปัญญาประดิษฐ์ (AI) มาใช้แต่ไม่มีการสร้างความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์จากการใช้ ปัญญาประดิษฐ์ของบุคลากร (สืบค้นจาก www.ncsa.or.th/policy/threat-statistics 14 ธันวาคม 2568)

โรงพยาบาลโดยเฉพาะโรงพยาบาลของรัฐ จำเป็นที่ต้องปฏิบัติตามกฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ดังเช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ รวมถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล โดยเฉพาะข้อมูลส่วนบุคคลเกี่ยวกับผู้ป่วยที่มีการเก็บรวบรวมไว้ในโรงพยาบาลถือว่าเป็นข้อมูลที่มีระดับความเสี่ยงต่อจิตใจหากหลุดรั่วไหล หรือถูกเข้าถึงและนำไปใช้โดยไม่ได้รับอนุญาต การป้องกันข้อมูลรั่วไหลจึงเป็นส่วนสำคัญในด้านความมั่นคงปลอดภัยที่โรงพยาบาลต้องตระหนักและป้องกันไม่ให้เกิดเหตุ

โรงพยาบาล ถือเป็นหน่วยงานที่ให้การรักษา ให้คำปรึกษาแก่ผู้ป่วยทั้งที่มีอาการเบาไปจนอาการหนักต้องพักรักษาตัวข้ามคืน ซึ่งคำนิยามของโรงพยาบาลที่สำนักสถิติแห่งชาติได้ให้ไว้คือ โรงพยาบาลหมายถึงสถานพยาบาลใด ซึ่งได้รับอนุญาตให้ดำเนินการรักษาคนไข้หรือผู้ป่วย ซึ่งจะมีเตียงค้างคืน หรือเพื่อการวินิจฉัยโรค การศัลยกรรม ผ่าตัด และให้การพยาบาลเต็มเวลา (สำนักงาน

สถิติแห่งชาติ) ซึ่งถือเป็นหน่วยงานที่มีความสำคัญอย่างมากด้วยภาระกิจความรับผิดชอบต่อชีวิตโดยตรง มีการเก็บประวัติการรักษา ประวัติข้อมูลส่วนบุคคลทั้งข้อมูลทั่วไปข้อมูลอ่อนไหวรวมถึงข้อมูลบุคคลสำคัญและข้อมูลบุคคลที่สาม ปัจจุบันมีสถานพยาบาลในประเทศไทยมีจำนวนมากถึง 11,940 แห่ง แบ่งเป็นโรงพยาบาลขนาดใหญ่หรือโรงพยาบาลศูนย์จำนวน 29 แห่ง โรงพยาบาลทั่วไปจำนวน 68 แห่ง และโรงพยาบาลทั่วไป โรงพยาบาลชุมชนจำนวน 11,843 แห่ง (ข้อมูล ณ วันที่ 25 สิงหาคม 2567) (สืบค้นจาก <https://www.thaicarecloud.org/report-cocs/show-overview,2567>) ปัจจุบันสถานพยาบาลแต่ละแห่งมีการพัฒนานวัตกรรมเทคโนโลยีใหม่ ๆ เข้ามาปรับใช้ในการให้บริการทั้งด้านการรักษาพยาบาล การให้คำปรึกษา การรักษาและให้คำปรึกษาโดยผ่านเครือข่ายสื่อสารทางไกล (Internet) รวมถึงอุปกรณ์ทางการแพทย์ที่มีนวัตกรรมหุ่นยนต์เข้ามาให้บริการ รวมถึงการนำอุปกรณ์ให้บริการเครือข่าย (Networking) อุปกรณ์ป้องกันเครือข่าย (Network Security) และการป้องกันภัยคุกคามทางไซเบอร์ ซึ่งเหล่านี้หากไม่มีการดูแลด้านความมั่นคงปลอดภัย การปรับปรุงประสิทธิภาพด้านเทคโนโลยีก็จะเป็นช่องโหว่ที่ผู้ที่ต้องลักลอบเจาะระบบ (Hacker) ใช้เป็นช่องทางในการเข้าถึงระบบงานสำคัญหรือแฝงเข้ามาลักลอบนำข้อมูลสำคัญออกไปใช้ในทางที่ผิด รวมถึงทำให้เกิดความเสียหายต่อระบบนวัตกรรมและเทคโนโลยีสารสนเทศได้ ดังเช่นเหตุการณ์ที่โรงพยาบาลถูกโจมตีจากภัยคุกคามทางไซเบอร์ ไม่ว่าจะเป็นการลักลอบเจาะข้อมูล หรือโจมตีด้วยไวรัสเรียกค่าไถ่ (Ransomware) ทำให้เกิดความผลกระทบถึง 40,000 คน และเกิดความเสียหายต่อระบบเก็บข้อมูลประวัติการรักษา และแม้ว่าจะมีประกาศนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกระทรวงสาธารณสุข พ.ศ. 2565 เมื่อเมษายน พ.ศ. 2565 (สำนักปลัดกระทรวงสาธารณสุข, 2565) ก็ยังพบว่า รายงานสถิติหน่วยงานที่ถูกโจมตีทางไซเบอร์ปี พ.ศ. 2568 พบว่า หน่วยงานด้านสาธารณสุขอยู่อันดับที่ 6 ของหน่วยงานทั้งหมดที่ถูกโจมตีทางไซเบอร์ (สำนักงานสถิติแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2568) และจากที่สำนักงานคุ้มครองข้อมูลส่วนบุคคล (สคส.) ให้สำนักปลัดกระทรวงสาธารณสุขเข้าชี้แจงประเด็นข้อมูลส่วนบุคคลรั่วไหลไปอยู่ใน Dark Web (สำนักงานคุ้มครองข้อมูลส่วนบุคคล, 2567) แม้จะมีการชี้แจงว่าไม่ได้เป็นข้อมูลทั่วไปและไม่ได้มาจากกระทรวงสาธารณสุข แต่อย่างไรก็ต้องมีการเฝ้าระวังและมาตรการในการป้องกัน รวมถึงการปรับปรุงเทคโนโลยีที่ใช้ในการป้องกันให้มีประสิทธิภาพ รวมถึงการนำมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ เช่น HAIT Plus, ISO 27001 และกระบวนการการตรวจประเมินช่องโหว่ ทดสอบเจาะระบบ รวมถึงการพัฒนาบุคลากรให้มีความรู้ในการป้องกันภัยทางไซเบอร์ (สืบค้นจาก <https://www.hfocus.org/content/2024/03/30032,2567>)

จากสาเหตุดังกล่าว ทำให้ผู้วิจัยเล็งเห็นถึงความสำคัญของการป้องกันภัยจากการโจมตีทางไซเบอร์ ทั้งด้านบุคลากรที่มีส่วนเกี่ยวข้อง กระบวนการในการจัดการโดยปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ที่เกี่ยวข้อง และด้านเทคโนโลยีในการเพิ่มประสิทธิภาพ การเลือกใช้เทคโนโลยีในการป้องกันอย่างเหมาะสมในการป้องกันภัยทางไซเบอร์สำหรับสถานพยาบาลได้อย่างมีประสิทธิภาพ

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อศึกษาการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ของผู้บริหารโรงพยาบาล ได้แก่ ผู้บริหารโรงพยาบาล ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ผู้บริหารด้านคุณภาพโรงพยาบาล ผู้บริหารฝ่ายการพยาบาล และบุคลากรของโรงพยาบาล

1.2.2 เพื่อวิเคราะห์ปัจจัยที่มีอิทธิพลต่อการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล ตามแนวทางของ HAIT Plus และ ISO/IEC 27001:2022

1.3 สมมติฐานของการวิจัย

จากการทบทวนวรรณกรรม เกี่ยวกับการวิเคราะห์ปัจจัยการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาลและงานวิจัยที่เกี่ยวข้อง ได้กำหนดสมมติฐานเพื่อตอบวัตถุประสงค์ของการวิจัยไว้ ดังนี้

1.3.1 สมมติฐานที่ 1 (H1) ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลเชิงบวกต่อการรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (Perceived Usefulness: PU) ของมาตรการ/มาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ

1.3.2 สมมติฐานที่ 2 (H2) ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลเชิงบวกต่อความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) ของมาตรการ/มาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ

1.3.3 สมมติฐานที่ 3 (H3) ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลเชิงบวกต่อความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) ของมาตรการ/มาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ

1.4 ขอบเขตของการวิจัย

ผู้วิจัยได้กำหนดขอบเขตของการวิจัยในครั้งนี้ เพื่อให้การศึกษาสามารถดำเนินการได้สำเร็จ ล่วงภายใต้ข้อจำกัดด้านทรัพยากรและเวลา โดยมีรายละเอียดดังต่อไปนี้

1.4.1 ขอบเขตด้านเนื้อหา

การวิจัยนี้มุ่งศึกษา แนวคิดเกี่ยวกับปัจจัยการรับรู้มาตรฐานความมั่นคงทางไซเบอร์ของโรงพยาบาล HAIT Plus ด้านมาตรฐานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ISO/IEC 27001:2022 และความสอดคล้องระหว่างมาตรฐานทั้งสอง

1.4.2 ขอบเขตด้านประชากรและกลุ่มตัวอย่าง

1.4.2.1 ประชากรที่ทำการศึกษาวิจัยครั้งนี้ คือ บุคลากรของโรงพยาบาลธรรมศาสตร์เฉลิมพระเกียรติ

1.4.2.2 กลุ่มตัวอย่าง (Sample) กลุ่มตัวอย่างที่ใช้ในการวิจัย คือ บุคลากรของโรงพยาบาลธรรมศาสตร์เฉลิมพระเกียรติ โดยกำหนดขนาดกลุ่มตัวอย่างเป้าหมายไว้ที่ประมาณ 250

คน และใช้วิธีการเลือกกลุ่มตัวอย่างแบบเฉพาะเจาะจง (Purposive Sampling) และแบบสะดวก (Convenience Sampling) แบ่งเป็น

1.4.2.2.1 กลุ่มผู้บริหารโรงพยาบาล ได้แก่ ผู้บริหารโรงพยาบาล ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ผู้บริหารด้านคุณภาพโรงพยาบาล ผู้บริหารฝ่ายการพยาบาล

1.4.2.2.2 กลุ่มเจ้าหน้าที่ผู้ปฏิบัติงานในโรงพยาบาล

1.4.3 ขอบเขตด้านเครื่องมือ

1.4.3.1 เครื่องมือที่ใช้ในการศึกษาการวิจัยเชิงสำรวจ (Survey Research Method) ในครั้งนี้ คือแบบสอบถามออนไลน์โดยใช้ Google Forms

1.4.3.2 การวิเคราะห์ข้อมูลในงานวิจัยนี้ใช้โปรแกรม Jamovi และ SmartPLS ซึ่งเป็นเครื่องมือทางสถิติที่ได้รับความนิยมในการวิจัยเชิงปริมาณด้านสังคมศาสตร์ โดยทั้งสองโปรแกรมมีบทบาทแตกต่างกันในการสนับสนุนการวิเคราะห์ข้อมูลในแต่ละขั้นตอน ดังนี้

1.4.4 การเก็บรวบรวมข้อมูล

ใช้แบบสอบถามออนไลน์ Google Forms ในการเก็บรวบรวมข้อมูล โดยการใช้การแจกแบบสอบถามผ่านช่องทางออนไลน์ Facebook Messenger และ Line Application

1.4.6 สถิติที่ใช้ในงานวิจัย

1.4.6.1 สถิติเชิงพรรณนา (Descriptive Statistics) สถิติเชิงพรรณนา (Descriptive Statistics) ใช้เพื่ออธิบายลักษณะทั่วไปของกลุ่มตัวอย่างและระดับความคิดเห็นของผู้ตอบแบบสอบถาม โดยประกอบด้วย ค่าเฉลี่ย (Mean) ค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation: SD) ค่าความแปรปรวน (Variance) สถิติดังกล่าวใช้ในการวิเคราะห์ข้อมูลพื้นฐาน และอธิบายแนวโน้มเข้าสู่ส่วนกลางและการกระจายของข้อมูลจากแบบสอบถาม เพื่อสะท้อนระดับความคิดเห็นเกี่ยวกับ ปัจจัยการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล

1.4.6.2 สถิติเชิงอนุมาน (Inferential Statistics) ใช้ในการทดสอบสมมติฐานและตรวจสอบความสัมพันธ์ระหว่างตัวแปรตามกรอบแนวคิดการวิจัย โดยประกอบด้วย

1.4.6.2.1 การวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmatory Factor Analysis: CFA) เพื่อทดสอบความตรงเชิงโครงสร้างของตัวแปรแฝง

1.4.6.2.2 การวิเคราะห์โมเดลสมการโครงสร้าง (Structural Equation Modeling: SEM) เพื่อทดสอบอิทธิพลเชิงสาเหตุระหว่างตัวแปรอิสระ ความตั้งใจเชิงพฤติกรรม และพฤติกรรมการใช้งานจริง

1.5 ตัวแปรที่ศึกษา

1.5.1 ตัวแปรอิสระหรือตัวแปรต้น (Independent Variable) จำนวน 2 ตัว ได้แก่

1.5.1.1 ปัจจัยด้านความพร้อมเทคโนโลยีสารสนเทศ

1.5.1.1.1 ปัจจัยด้านนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

1.5.1.1.2 ปัจจัยด้านการปฏิบัติตามกฎหมายหรือระเบียบปฏิบัติ

1.5.1.1.3 ปัจจัยด้านความพร้อมของอุปกรณ์หรือระบบ

1.5.1.1.4 ปัจจัยด้านงบประมาณ

1.5.1.1.5 ปัจจัยด้านแนวทางการพัฒนา

1.5.1.2 ปัจจัยด้านบุคลากร

1.5.1.2.1 ปัจจัยด้านนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

1.5.1.2.2 ปัจจัยด้านการปฏิบัติตามกฎหมายหรือระเบียบปฏิบัติ

1.5.2 ตัวแปรตาม (Dependent Variable) จำนวน 2 ตัว ได้แก่

1.5.2.1 ปัจจัยด้านความพร้อมในการพัฒนาการบริหารด้านความมั่นคงปลอดภัยทาง

ไซเบอร์

1.5.2.1.1 ปัจจัยด้านมาตรฐาน HAIT Plus

1.5.2.1.2 ปัจจัยด้านมาตรฐาน ISO/IEC 27001:2022

1.5.2.2 ปัจจัยด้านการรับรู้ความมั่นคงปลอดภัยทางไซเบอร์โรงพยาบาล

1.5.2.2.1 ปัจจัยด้านการรับรู้ข้อกำหนดมาตรฐาน

1.5.2.2.2 ปัจจัยด้านการรับรู้ภัยคุกคามทางไซเบอร์

1.6 นิยามศัพท์เฉพาะ

เพื่อให้เกิดความเข้าใจตรงกันในการวิจัยครั้งนี้ ผู้วิจัยได้กำหนดนิยามศัพท์เฉพาะที่ใช้ในการวิจัยไว้ดังต่อไปนี้

1.6.1 ความมั่นคงปลอดภัยทางไซเบอร์ หมายถึง ระบบการป้องกัน การสร้างความมั่นคงปลอดภัยให้กับข้อมูลสารสนเทศที่มีการใช้งานอยู่ การป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การดัดแปลง หรือการทำลาย ซึ่งเป็นสาเหตุที่ทำให้ไม่สามารถใช้งานข้อมูลสารสนเทศได้ โดยมีหลักสำคัญ 3 ประการ คือ การรักษาความลับ (Confidentiality) การรักษาความครบถ้วนสมบูรณ์ (Integrity) และการรักษาความพร้อมใช้งาน (Availability)

1.6.2 โรงพยาบาล หมายถึง สถานที่รวมตลอดถึงยานพาหนะที่มีเตียงรับคนไข้ไว้ค้างคืน ซึ่งจัดไว้เพื่อการประกอบโรคศิลปะตามกฎหมายว่าด้วยการควบคุมการประกอบโรคศิลปะ หรือกิจการอื่นด้วยการผ่าตัด ฉีดยา หรือด้วยการใช้กรรมวิธีอื่นซึ่งเป็นกรรมวิธีการประกอบโรคศิลปะ ทั้งนี้โดยกระทำเป็นปกติธุระไม่ว่าจะได้รับผลประโยชน์ตอบแทนหรือไม่ และเป็นสถานพยาบาลซึ่งได้รับอนุญาตให้ตั้งและดำเนินการตาม พ.ร.บ. สถานพยาบาล พ.ศ. 2541 และสถานพยาบาลโพลีคลินิก ทั้งนี้ไม่รวมสถานพยาบาลซึ่งมีประกาศกระทรวงสาธารณสุขให้ได้รับการยกเว้นตาม พ.ร.บ. สถานพยาบาล พ.ศ. 2541

1.6.3 มาตรฐาน HAIT Plus แนวทางการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับโรงพยาบาล เกิดจากความร่วมมือของสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ สกมช. และสมาคมเวชสารสนเทศไทย (Thai Medical Informatics Association – TMI) โดยมีวัตถุประสงค์เพื่อให้โรงพยาบาลได้มีแนวทางพัฒนาระบบความมั่นคงปลอดภัยไซเบอร์ให้เกิดขึ้น ตามกฎหมาย และแนวทางปฏิบัติที่เกี่ยวข้อง และยกระดับให้มีความปลอดภัยเพิ่มขึ้นอย่างต่อเนื่อง

1.6.4 มาตรฐาน ISO/IEC 27001 หมายถึง แนวทาง ระบบการบริหารจัดการ และกระบวนการที่เกี่ยวข้องกับ อุปกรณ์ ระบบเทคโนโลยีสารสนเทศ กลุ่มบุคคล และแนวทางการป้องกันความเสี่ยงอย่างถูกต้องและได้ประสิทธิภาพ ด้วย 3 หลักสำคัญ คือ การป้องกันการเข้าถึงข้อมูลเฉพาะผู้ที่ได้รับอนุญาต การปกป้องความครบถ้วนและถูกต้องของข้อมูล และความพร้อมใช้ของข้อมูล

1.7 ประโยชน์ที่คาดว่าจะได้รับ

จากการดำเนินการวิจัยในครั้งนี้ ผู้วิจัยคาดว่าจะได้รับประโยชน์ที่สำคัญทั้งในเชิงวิชาการและเชิงปฏิบัติ ดังนี้

1.7.1 งานวิจัยนี้ช่วยขยายองค์ความรู้ด้านการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ในบริบทของโรงพยาบาล โดยบูรณาการแนวคิดมาตรฐาน HAIT Plus และ ISO/IEC 27001:2022 เข้ากับกรอบการวิเคราะห์เชิงปริมาณ (PLS-SEM) ทำให้เกิดแบบจำลองเชิงสาเหตุที่สามารถอธิบายปัจจัยที่มีอิทธิพลต่อการรับรู้และความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างเป็นระบบ

1.7.2 ผลการวิจัยสามารถใช้เป็นข้อมูลสนับสนุนผู้บริหารโรงพยาบาลในการกำหนดนโยบาย กลยุทธ์ และแผนพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับมาตรฐานสากลและข้อกำหนดทางกฎหมาย อันจะช่วยยกระดับธรรมาภิบาลด้านข้อมูล (Data Governance) และการบริหารความเสี่ยงขององค์กร

1.7.3 โรงพยาบาลสามารถนำผลการวิจัยไปใช้เป็นแนวทางประเมินระดับความพร้อมด้านเทคโนโลยี บุคลากร และกระบวนการ เพื่อปรับปรุงระบบป้องกันภัยคุกคามไซเบอร์ ลดความเสี่ยงจากการโจมตี การรั่วไหลของข้อมูล และเหตุการณ์ด้านความมั่นคงปลอดภัยที่อาจส่งผลกระทบต่อผู้ป่วยและองค์กร

1.7.4 ผลการศึกษาเกี่ยวกับการรับรู้และความเข้าใจมาตรฐานความมั่นคงปลอดภัยไซเบอร์สามารถใช้เป็นแนวทางในการออกแบบหลักสูตรฝึกอบรมและพัฒนาความตระหนักรู้ด้านไซเบอร์ซีเคียวริตี้สำหรับผู้บริหารและบุคลากรในโรงพยาบาล เพื่อเสริมสร้างวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์อย่างยั่งยืน

1.7.5 แบบจำลองและเครื่องมือวัดที่พัฒนาขึ้นในงานวิจัยนี้สามารถนำไปประยุกต์ใช้หรือขยายผลในบริบทของสถานพยาบาลประเภทอื่น หรือหน่วยงานภาครัฐและเอกชนที่มีการจัดการข้อมูลอ่อนไหว เพื่อเปรียบเทียบผลลัพธ์และพัฒนาองค์ความรู้ด้านการบริหารความมั่นคงปลอดภัยไซเบอร์ในระดับที่กว้างขึ้น

บทที่ 2

เอกสารและงานวิจัยที่เกี่ยวข้อง

งานวิจัยนี้จัดทำขึ้นเพื่อศึกษาวิเคราะห์ปัจจัยการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล โดยผู้วิจัยได้ศึกษาและค้นคว้าจากข้อมูล แนวคิด ทฤษฎี และงานวิจัยต่าง ๆ ที่เกี่ยวข้อง เพื่อนำมาใช้เป็นข้อมูลการกำหนดสมมติฐาน และออกแบบเครื่องมือที่ใช้ในงานวิจัยในบทต่อไป ดังนั้น เพื่อเป็นแนวทางในการศึกษาวิจัย ผู้วิจัยได้นำเสนอเนื้อหาที่เกี่ยวข้องกับการวิจัยดังต่อไปนี้

- 2.1 มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์
- 2.2 มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล
- 2.3 ขอบกฎหมาย ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับโรงพยาบาล
- 2.4 ทฤษฎีปัจจัยด้านการรับรู้และพฤติกรรมของบุคลากร
- 2.5 ทฤษฎีที่เกี่ยวข้องกับการยอมรับเทคโนโลยีสารสนเทศ
- 2.6 งานวิจัยที่เกี่ยวข้อง

2.1 มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์

มาตรฐาน ISO/IEC 27001:2022 เป็นมาตรฐานสากลด้านระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ภายใต้ชื่อ Information security, cybersecurity and privacy protection - Information security management systems ประกาศใช้เมื่อวันที่ 10 ตุลาคม พ.ศ. 2565 โดยเป็นการปรับปรุงจากฉบับเดิมคือ ISO/IEC 27001:2013 เพื่อให้สอดคล้องกับบริบทภัยคุกคามไซเบอร์ที่เปลี่ยนแปลงอย่างรวดเร็ว เทคโนโลยีดิจิทัลที่มีความซับซ้อนมากขึ้น และข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคลในระดับสากล (ISO, 2022)

มาตรฐานฉบับปี 2022 มีวัตถุประสงค์เพื่อกำหนดกรอบการบริหารจัดการที่เป็นระบบในการรักษา ความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลสารสนเทศ โดยใช้แนวคิดการบริหารความเสี่ยง (Risk-based approach) เป็นกลไกหลักในการวิเคราะห์ ประเมิน และกำหนดแนวทางควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม

แนวคิดดังกล่าวมีความสอดคล้องกับหลักการบริหารความเสี่ยงตาม ISO 31000 ซึ่งเน้นการระบุ วิเคราะห์ ประเมิน และจัดการความเสี่ยงอย่างเป็นระบบ โปร่งใส และสามารถตรวจสอบได้ (ISO, 2018) โดย ISO/IEC 27001 นำหลักการดังกล่าวมาประยุกต์ใช้ในบริบทด้านสารสนเทศและไซเบอร์โดยเฉพาะ

2.1.1 โครงสร้างและสาระสำคัญของ ISO/IEC 27001:2022

ISO/IEC 27001:2022 ใช้โครงสร้างตาม Annex SL ซึ่งเป็นโครงสร้างมาตรฐานเดียวกับมาตรฐานระบบบริหารอื่น ๆ เพื่อให้สามารถบูรณาการร่วมกันได้ โดยมีข้อกำหนดหลักตั้งแต่ข้อ 4–10 ดังนี้

ข้อ 4 บริบทขององค์กร (Context of the Organization) องค์กรต้องกำหนดบริบททั้งภายในและภายนอก ระบุผู้มีส่วนได้เสีย (Interested Parties) และความคาดหวังที่เกี่ยวข้อง จากนั้นกำหนดขอบเขตของ ISMS ให้ชัดเจนและเป็นลายลักษณ์อักษร เพื่อให้การดำเนินงานมีขอบเขตที่ตรวจสอบได้

ข้อ 5 ภาวะผู้นำ (Leadership) ผู้บริหารระดับสูงต้องแสดงบทบาทความเป็นผู้นำอย่างชัดเจน ได้แก่ การกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ การบูรณาการ ISMS เข้ากับกระบวนการหลักขององค์กร การจัดสรรทรัพยากรอย่างเพียงพอ การกำหนดบทบาท หน้าที่ และความรับผิดชอบ การสนับสนุนการปรับปรุงอย่างต่อเนื่อง สาระสำคัญในข้อนี้สะท้อนว่า ISMS มิใช่ภารกิจของฝ่ายเทคโนโลยีสารสนเทศเพียงลำพัง แต่เป็นความรับผิดชอบเชิงกลยุทธ์ขององค์กรทั้งหมด

ข้อ 6 การวางแผน (Planning: Risk-Based Approach) องค์กรต้องจัดให้มี การประเมินความเสี่ยง (Risk Assessment) การจัดการความเสี่ยง (Risk Treatment) กระบวนการดังกล่าวต้องสามารถทำซ้ำได้ มีเกณฑ์ประเมินที่ชัดเจน และมีเอกสารหลักฐานรองรับ ผลการจัดการความเสี่ยงต้องเชื่อมโยงกับรายการควบคุมในภาคผนวก Annex A พร้อมจัดทำเอกสาร Statement of Applicability (SoA) เพื่อแสดงเหตุผลในการเลือกหรือไม่เลือกมาตรการควบคุมแต่ละข้ออย่างโปร่งใสและตรวจสอบได้

ข้อ 7–10 การสนับสนุน การดำเนินการ การประเมินผล และการปรับปรุง ข้อกำหนดในส่วนนี้มุ่งเน้นให้ระบบสามารถนำไปปฏิบัติได้จริงและเกิดการพัฒนายอย่างต่อเนื่อง ได้แก่ การพัฒนาความสามารถและความตระหนักรู้ของบุคลากร (Competence & Awareness) การควบคุมเอกสารและสารสนเทศ การควบคุมการปฏิบัติงาน (Operational Control) การติดตาม ตรวจสอบ และประเมินผล (Monitoring & Measurement) การตรวจติดตามภายใน (Internal Audit) การทบทวนโดยฝ่ายบริหาร (Management Review) การดำเนินการแก้ไขและปรับปรุงอย่างต่อเนื่อง (Corrective Action & Continual Improvement) โครงสร้างดังกล่าวสะท้อนวงจรการบริหารแบบ PDCA (Plan–Do–Check–Act) ซึ่งช่วยให้ ISMS ไม่เป็นเพียงเอกสารเชิงนโยบาย แต่เป็นระบบบริหารที่มีการวัดผลและปรับปรุงอย่างเป็นรูปธรรม

2.1.2 ภาคผนวก Annex A และแนวคิดการควบคุม ISO/IEC 27001:2022 ได้ปรับโครงสร้างรายการควบคุมใน Annex A ให้แบ่งออกเป็น 4 หมวดหลัก ได้แก่

2.1.2.1 การควบคุมด้านองค์กร (Organizational Controls)

2.1.2.2 การควบคุมด้านบุคลากร (People Controls)

2.1.2.3 การควบคุมด้านกายภาพ (Physical Controls)

2.1.2.4 การควบคุมด้านเทคโนโลยี (Technological Controls)

แนวทางดังกล่าวสะท้อนมุมมองเชิงบูรณาการที่ครอบคลุมทั้งมิติด้านโครงสร้างองค์กร พฤติกรรมมนุษย์ สภาพแวดล้อมทางกายภาพ และเทคโนโลยีสารสนเทศ ซึ่งสอดคล้องกับแนวคิดด้าน ปัจจัยมนุษย์ (Human Factors) ในการบริหารความมั่นคงปลอดภัยไซเบอร์

2.1.3 ความสำคัญต่อวงการวิชาการและบริบทโรงพยาบาล

ในเชิงวิชาการ ISO/IEC 27001 เป็นกรอบมาตรฐานที่เอื้อต่อการวิจัยด้านการบริหารความเสี่ยงและความพร้อมด้านไซเบอร์ เนื่องจากมีโครงสร้างตัวชี้วัด กระบวนการตรวจประเมิน และหลักฐานเชิงเอกสารที่ชัดเจน ทำให้งานวิจัยสามารถกำหนดตัวแปร วัดผล และเปรียบเทียบผลการดำเนินงานได้อย่างเป็นระบบ ในบริบทของโรงพยาบาล ความสำคัญของมาตรฐานดังกล่าวยิ่งทวีความชัดเจน เนื่องจาก

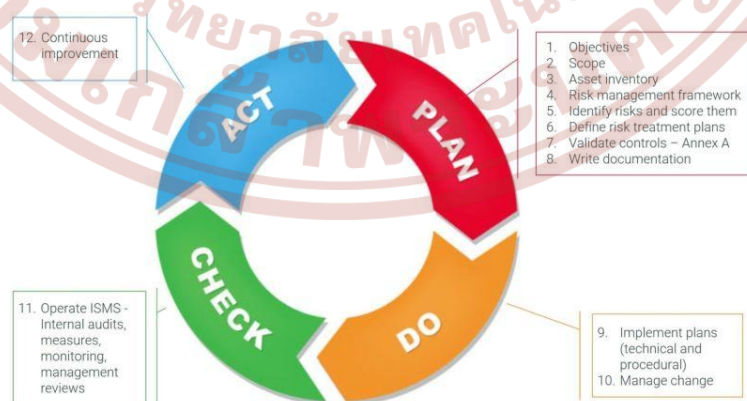
2.1.3.1 มีการจัดเก็บข้อมูลสุขภาพและข้อมูลส่วนบุคคลที่มีความอ่อนไหวสูง

2.1.3.2 ต้องรักษาความพร้อมใช้งานของระบบอย่างต่อเนื่อง เนื่องจากเกี่ยวข้องโดยตรงกับความปลอดภัยของผู้ป่วย

2.1.3.3 มีการพึ่งพาผู้ให้บริการระบบสารสนเทศและผู้จำหน่ายภายนอกจำนวนมาก

มาตรการควบคุมใน Annex A เช่น การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (Incident Management) การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity) การสำรองข้อมูล (Backup) การบันทึกและเฝ้าระวังเหตุการณ์ (Logging & Monitoring) ตลอดจนการบริหารความสัมพันธ์กับผู้ส่งมอบ (Supplier Relationship Security) จึงมีความสอดคล้องกับความเสี่ยงเฉพาะขององค์กรด้านสาธารณสุขอย่างมีนัยสำคัญ

2.1.4 แนวคิดหลัก PDCA (Plan-Do-Check-Act) เป็นหลักการบริหารจัดการที่มุ่งเน้นการพัฒนาอย่างต่อเนื่อง (Continual Improvement) และถูกนำมาใช้เป็นโครงสร้างสำคัญของระบบบริหารจัดการตาม ISO/IEC 27001:2022 โดยกำหนดให้ทุกกระบวนการของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ดำเนินไปอย่างเป็นระบบ ตรวจสอบได้ และสามารถปรับปรุงอย่างต่อเนื่อง



ภาพที่ 2-1 แสดงแนวคิดหลัก PDCA

ที่มา: เอกสารประกอบการอบรม ISO/IEC 27001:2022 Foundation.

ภายใต้ ISO/IEC 27001:2022 โครงสร้างข้อกำหนดข้อ 4-10 สามารถจัดวางตามแนวคิด PDCA ได้ดังนี้

2.1.4.1 บริบทขององค์กร (Context of the Organization) คือ องค์กรต้องทำความเข้าใจบริบททั้งภายในและภายนอก ระบุความต้องการและความคาดหวังของผู้มีส่วนได้เสีย กำหนดขอบเขตของ ISMS อย่างชัดเจน รวมถึงดำเนินการระบุและประเมินความเสี่ยงด้านสารสนเทศ เพื่อกำหนดแนวทางควบคุมและจัดการความเสี่ยงอย่างเหมาะสม ขั้นตอนดังกล่าวเป็นพื้นฐานสำคัญของการวางแผนเชิงระบบและการกำหนดทิศทางเชิงกลยุทธ์ขององค์กร

2.1.4.2 ภาวะผู้นำ (Leadership) คือ ฝ่ายบริหารระดับสูงต้องแสดงความมุ่งมั่นและความรับผิดชอบต่อระบบ ISMS โดยกำหนดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ จัดสรรทรัพยากร กำหนดบทบาท อำนาจหน้าที่ และความรับผิดชอบอย่างชัดเจน ตลอดจนสนับสนุนการบูรณาการ ISMS เข้ากับกระบวนการหลักขององค์กร

2.1.4.3 การวางแผน (Planning) คือ องค์กรต้องจัดทำแผนบริหารจัดการความเสี่ยงและโอกาส (Risk and Opportunity Management) กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ และจัดทำแผนรองรับการเปลี่ยนแปลง (Change Planning) เพื่อให้มั่นใจว่าระบบสามารถปรับตัวต่อสภาพแวดล้อมที่เปลี่ยนแปลงได้อย่างเหมาะสม

2.1.4.3 การสนับสนุน (Support) คือ องค์กรต้องจัดสรรทรัพยากรที่จำเป็นต่อการดำเนินงานของ ISMS ครอบคลุมการกำหนดสมรรถนะบุคลากร การสร้างความตระหนักรู้ การฝึกอบรมและการซ้อมแผน การสื่อสารภายในองค์กร ตลอดจนการจัดทำและควบคุมเอกสารและบันทึกที่เกี่ยวข้อง

2.1.4.4 การดำเนินการ (Operation) เป็นขั้นตอนการนำแผนไปสู่การปฏิบัติ ครอบคลุมการควบคุมการดำเนินงาน การประเมินความเสี่ยงอย่างต่อเนื่อง และการดำเนินการจัดการความเสี่ยงตามแผนที่กำหนดไว้

2.1.4.5 การประเมินผลการดำเนินงาน (Performance Evaluation) องค์กรต้องมีการเฝ้าระวัง การวัดผล การวิเคราะห์ และการประเมินผลการดำเนินงาน เปรียบเทียบกับข้อกำหนดของ ISMS รวมถึงการตรวจติดตามภายใน (Internal Audit) และการทบทวนโดยฝ่ายบริหาร (Management Review) เพื่อประเมินความเพียงพอและประสิทธิผลของระบบ

2.1.4.6 การปรับปรุงอย่างต่อเนื่อง หรือ Continual improvement คือ การปรับปรุงความเหมาะสม ความเพียงพอ และความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและข้อมูล (ISMS) อย่างต่อเนื่อง และดำเนินการกับความไม่สอดคล้อง (Non-conformance: NC) และการปฏิบัติการแก้ไข (Corrective action request)

2.1.4.7 การปรับปรุงอย่างต่อเนื่อง (Continual Improvement) คือ องค์กรต้องมีการเฝ้าระวัง การวัดผล การวิเคราะห์ และการประเมินผลการดำเนินงาน เปรียบเทียบกับข้อกำหนดของ ISMS รวมถึงการตรวจติดตามภายใน (Internal Audit) และการทบทวนโดยฝ่ายบริหาร (Management Review) เพื่อประเมินความเพียงพอและประสิทธิผลของระบบ

วงจร PDCA จึงทำหน้าที่เป็นกลไกที่ทำให้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศไม่หยุดอยู่เพียงระดับเอกสาร แต่เป็นระบบที่มีการวัดผล ทบทวน และพัฒนาอย่างต่อเนื่อง (ISO, 2022)

2.1.5 กรอบ NIST Cybersecurity Framework 2.0 เป็นกรอบแนวทางการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่พัฒนาโดย National Institute of Standards and Technology (NIST) แห่งสหรัฐอเมริกา มีวัตถุประสงค์เพื่อใช้เป็นแนวทางกลางสำหรับองค์กรทุกขนาดและทุกประเภทอุตสาหกรรม โดยเวอร์ชัน 2.0 ได้ปรับปรุงจากฉบับ 1.1 ให้มีความครอบคลุมองค์กรทุกภาคส่วน ไม่จำกัดเฉพาะโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Infrastructure) (NIST, 2024) จุดเด่นสำคัญของ CSF 2.0 คือ การเพิ่มองค์ประกอบ **Govern (GV)** เพื่อเน้นการกำกับดูแลและการเชื่อมโยงกับการบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management: ERM) ทำให้กรอบดังกล่าวมีมิติด้านกลยุทธ์และธรรมาภิบาลชัดเจนยิ่งขึ้น กรอบ NIST CSF 2.0 ประกอบด้วย 6 ฟังก์ชันหลัก ได้แก่ กรอบ NIST CSF 2.0 ประกอบด้วย 6 ฟังก์ชันหลัก ได้แก่

2.1.5.1 Govern (GV) คือ การกำกับดูแล กลยุทธ์ และนโยบาย เพื่อให้การบริหารความเสี่ยงไซเบอร์สอดคล้องกับบริบทและพันธกิจองค์กร

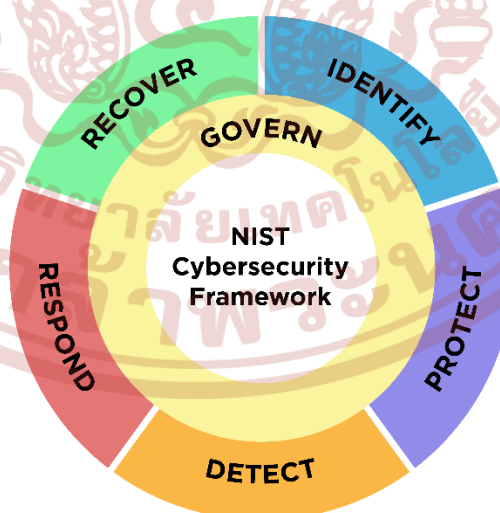
2.1.5.2 Identify (ID) คือ การระบุทรัพย์สิน บริบท และความเสี่ยง

2.1.5.3 Protect (PR) คือ การกำหนดและดำเนินมาตรการควบคุมเพื่อป้องกันระบบและข้อมูล

2.1.5.4 Detect (DE) คือ การเฝ้าระวังและตรวจจับเหตุการณ์ผิดปกติ

2.1.5.5 Respond (RS) คือ การตอบสนองเมื่อเกิดเหตุการณ์ด้านไซเบอร์

2.1.5.6 Recover (RC) คือ การฟื้นฟูระบบและข้อมูลให้กลับสู่สภาวะปกติ



ภาพที่ 2-2 กรอบ NIST Cybersecurity Framework 2.0

ที่มา: เอกสารประกอบการสัมมนาความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาลรัฐ

ความสำคัญของ NIST CSF 2.0 ต่อบริบทโรงพยาบาล กรอบ CSF 2.0 สามารถใช้เป็นเครื่องมือประเมินระดับความพร้อม (Cybersecurity Maturity Assessment) และการวิเคราะห์ช่องว่าง (Gap Analysis) ได้อย่างเป็นระบบ เนื่องจากแต่ละ Subcategory มีลักษณะเป็นผลลัพธ์เชิงการจัดการ ความเสี่ยงที่ตรวจสอบได้ สำหรับโรงพยาบาลซึ่งมีระบบที่เกี่ยวข้องกับชีวิตและความปลอดภัยของผู้ป่วย การหยุดชะงักของระบบสารสนเทศอาจส่งผลกระทบรุนแรงกว่าภาคธุรกิจทั่วไป การนำ CSF 2.0 มาประยุกต์ใช้จึงช่วยให้สามารถกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite/Tolerance) เชื่อมโยงกับการบริหารความเสี่ยงระดับองค์กร และกำหนดกลไกกำกับดูแลที่ชัดเจน ตัวอย่างแนวทางเชื่อมโยงกับ ISO/IEC 27001 และมาตรฐานด้านสาธารณสุข เช่น HAIT Plus ได้แก่

- 1 Govern (GV) บริบท พันธกิจ บริการที่สำคัญ ข้อกฎหมายและสัญญา (GV.OC)
- 2 Risk appetite/tolerance และ Enterprise risk management (GV.RM)
- 3 การกำหนดบทบาท อำนาจหน้าที่ ทรัพยากรผู้นำ ภาวะผู้นำ (GV. RR)
- 4 การทบทวนนโยบาย (GV.PO) และ ระบบกำกับติดตาม (GV.OV)
- 5 การจัดการความเสี่ยง Supply Chain (GV.SC)

ดังนั้น การบูรณาการแนวคิด PDCA ของ ISO/IEC 27001 เข้ากับกรอบ Govern-Identify-Protect-Detect-Respond-Recover ของ NIST CSF 2.0 จะช่วยให้องค์กร โดยเฉพาะโรงพยาบาล สามารถยกระดับการบริหารความมั่นคงปลอดภัยไซเบอร์จากระดับการปฏิบัติการสู่ระดับกลยุทธ์และธรรมาภิบาลองค์กรได้อย่างเป็นระบบและยั่งยืน

2.2 มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล

แนวทางการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับโรงพยาบาลของรัฐ (HAIT Plus) เป็นกรอบมาตรฐานเฉพาะบริบทของหน่วยบริการสาธารณสุขภาครัฐในประเทศไทย ที่พัฒนาขึ้นเพื่อบูรณาการข้อกำหนดตามกฎหมายไทยและมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศเข้าด้วยกัน โดยมีเป้าหมายเพื่อยกระดับความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลให้มีความมั่นคง ยั่งยืน และสอดคล้องกับความเสี่ยงเฉพาะด้านสุขภาพ

แนวทางดังกล่าวครอบคลุมการบริหารจัดการใน 3 มิติหลัก ได้แก่ **People – Process – Technology** และมุ่งเน้นการบริหารความเสี่ยงในระบบสารสนเทศที่มีความสำคัญต่อการให้บริการรักษาพยาบาล เช่น ระบบ Hospital Information System (HIS) ระบบเวชระเบียนอิเล็กทรอนิกส์ (EMR/EHR) ระบบฐานข้อมูลผู้ป่วย และโครงสร้างพื้นฐานเครือข่ายสารสนเทศ

ในเชิงกฎหมาย แนวทาง HAIT Plus เชื่อมโยงกับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ตลอดจนสามารถบูรณาการกับมาตรฐานสากล เช่น ISO/IEC 27001:2022 และ NIST Cybersecurity Framework 2.0 เพื่อยกระดับระบบบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ในระดับองค์กร

2.2.1 องค์ประกอบหลักของ HAIT Plus องค์ประกอบสำคัญของแนวทาง HAIT Plus สามารถสรุปได้ดังนี้

2.2.1.1 Governance & Risk Management โรงพยาบาลต้องจัดทำนโยบายความมั่นคงปลอดภัยไซเบอร์อย่างเป็นลายลักษณ์อักษร กำหนดบทบาทและความรับผิดชอบของผู้บริหาร และหน่วยงานที่เกี่ยวข้อง รวมถึงดำเนินการประเมินความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ 1 ครั้ง เพื่อให้สามารถกำหนดมาตรการควบคุมที่เหมาะสมกับระดับความเสี่ยง

2.2.1.2 Data Protection & Privacy เน้นการคุ้มครองข้อมูลสุขภาพส่วนบุคคล (Personal Health Information: PHI) ให้สอดคล้องกับกฎหมาย PDPA และมาตรฐานสากล โดยครอบคลุมการจัดชั้นความลับข้อมูล การเข้ารหัสข้อมูล การกำหนดสิทธิ์การเข้าถึง และการควบคุมการเปิดเผยข้อมูล

2.2.1.3 Access Control & Authentication กำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศ เช่น การใช้การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) การกำหนดสิทธิ์ตามบทบาทหน้าที่ (Role-Based Access Control: RBAC) นโยบายรหัสผ่าน (Password Policy) ที่รัดกุมและสอดคล้องกับความเสี่ยง

2.2.1.4 Monitoring & Incident Response จัดให้มีระบบเฝ้าระวังและบันทึกเหตุการณ์ (Logging & Monitoring) พร้อมจัดทำแผนตอบสนองเหตุการณ์ (Incident Response Plan) และดำเนินการซ้อมแผนอย่างสม่ำเสมอ เพื่อให้สามารถควบคุมและจำกัดความเสียหายจากเหตุการณ์ไซเบอร์ได้อย่างทันท่วงที

2.2.1.5 Business Continuity & Disaster Recovery (BCP/DRP) กำหนดแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) และแผนกู้คืนระบบ (Disaster Recovery Plan: DRP) เพื่อรองรับกรณีระบบ HIS หรือ EMR ถูกโจมตีหรือเกิดเหตุขัดข้อง โดยต้องมีการทดสอบแผนและปรับปรุงอย่างต่อเนื่อง

2.2.1.6 Awareness & Training จัดให้มีการอบรมและสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์แก่บุคลากรทุกระดับอย่างต่อเนื่อง เนื่องจากบุคลากรถือเป็นปัจจัยสำคัญในการลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

2.2.1.7 Audit & Compliance ดำเนินการตรวจสอบและประเมินผลการปฏิบัติตามมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ตามรอบระยะเวลาที่กำหนด รวมถึงการประเมินความสอดคล้องกับข้อกำหนดทางกฎหมายและมาตรฐานที่เกี่ยวข้อง

2.2.2 มาตรการที่โรงพยาบาลต้องดำเนินการเพื่อให้การดำเนินงานเป็นรูปธรรม โรงพยาบาลของรัฐควรปฏิบัติตามมาตรการสำคัญ ดังนี้

2.2.2.1 การจัดทำทะเบียนทรัพย์สินสารสนเทศ ต้องจัดทำทะเบียนทรัพย์สินสารสนเทศ (Information Asset Inventory) ครอบคลุมฮาร์ดแวร์ ซอฟต์แวร์ ฐานข้อมูล และระบบสำคัญ พร้อมทบทวนและปรับปรุงอย่างน้อยปีละ 1 ครั้ง

2.2.2.2 การประเมินความเสี่ยงและการทดสอบเจาะระบบ ดำเนินการประเมินความเสี่ยงด้านสารสนเทศ และการทดสอบเจาะระบบ (Penetration Testing: Pentest) อย่างน้อยปีละ 1 ครั้ง เพื่อประเมินช่องโหว่และความพร้อมของระบบ

2.2.2.3 การจัดการบันทึกเหตุการณ์ (Log Management) จัดเก็บและบริหารจัดการข้อมูลจราจรทางคอมพิวเตอร์ให้เป็นไปตามข้อกำหนดของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พร้อมกำหนดระยะเวลาการจัดเก็บและการควบคุมการเข้าถึงข้อมูล Log อย่างเหมาะสม

2.2.2.4 การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) จัดตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) หรือผู้รับผิดชอบในการกำกับดูแลการจัดการข้อมูลผู้ป่วย เพื่อให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2.2.2.5 การบูรณาการกับมาตรฐานคุณภาพโรงพยาบาล บูรณาการแนวทาง HAIT Plus เข้ากับระบบรับรองคุณภาพโรงพยาบาล เช่น การรับรอง HA/NHA เพื่อให้การบริหารความมั่นคงปลอดภัยไซเบอร์เป็นส่วนหนึ่งของระบบคุณภาพโดยรวมขององค์กร

โดยสรุป แนวทาง HAIT Plus ทำหน้าที่เป็นกรอบปฏิบัติที่เชื่อมโยงกฎหมาย มาตรฐานสากล และบริบทเฉพาะของโรงพยาบาลไทยเข้าด้วยกัน ช่วยให้องค์กรสามารถยกระดับการบริหารความมั่นคงปลอดภัยไซเบอร์จากระดับเชิงเทคนิคสู่ระดับเชิงระบบและเชิงธรรมาภิบาลได้อย่างเป็นรูปธรรม และสอดคล้องกับความเสี่ยงที่มีความสำคัญต่อชีวิตและความปลอดภัยของผู้ป่วยโดยตรง

2.3 ข้อกำหนด ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับโรงพยาบาล

การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลในประเทศไทยอยู่ภายใต้กรอบกฎหมายและระเบียบข้อบังคับหลายฉบับ โดยเฉพาะกฎหมายที่เกี่ยวข้องกับการคุ้มครองโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) การคุ้มครองข้อมูลส่วนบุคคล และการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ

2.3.1 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 เป็นกรอบกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ มีการกำหนดมาตรการป้องกัน รับมือ และแก้ไขปัญหาคุกคามทางไซเบอร์ โดยมีวัตถุประสงค์ในการคุ้มครองหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) เช่น หน่วยงานพลังงาน หน่วยงานด้านการเงิน หน่วยงานคมนาคม รวมถึงหน่วยงานทางด้านสาธารณสุข ก็ถือเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือ CII เช่นกัน

โดยหน้าที่ของหน่วยงานหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จะต้องมีการจัดทำนโยบายและแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงและดำเนินการป้องกันภัยคุกคาม มีการรายงานเหตุการณ์หรือภัยคุกคามต่อ สกมช. และปฏิบัติตามมาตรการด้านการตรวจสอบ การฝึกอบรม และซักซ้อมแผนรับมือภัยคุกคาม ภายใต้มาตรการทางกฎหมายที่มีการแบ่งระดับภัยคุกคาม 3 ระดับ ได้แก่ 1) ไม่ร้ายแรง 2) ร้ายแรง และ 3) ร้ายแรงมาก ให้อำนาจเจ้าหน้าที่ในการสั่งการ ตรวจสอบ หรือระงับการใช้งานระบบสารสนเทศในบางกรณีได้ หากไม่ปฏิบัติหรือละเลยก็มีโทษทั้งทางปกครอง โทษทางอาญาสำหรับการไม่ปฏิบัติตามข้อกำหนด

หน่วยงานด้านสาธารณสุขถูกระบุชัดเจนว่าเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือ CII ครอบคลุมการให้บริการในโรงพยาบาล ระหว่างโรงพยาบาล ยา เวชภัณฑ์ การตรวจวิเคราะห์ ข้อมูลสุขภาพ โดยมีสำนักงานปลัดกระทรวงสาธารณสุขและหน่วยงานเกี่ยวข้องเป็น

ผู้กำกับดูแล ประกอบกับประกาศคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐาน สำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2564 หมวด 7 ด้าน สาธารณสุข โดยมีลักษณะหน่วยงาน คือ

ตารางที่ 2-1 โครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุข

ลักษณะหน่วยงาน	ภารกิจหรือให้บริการ (Critical Services)
1) เป็นหน่วยงานที่มีการ ให้บริการสุขภาพในโรงพยาบาล	1) บริการทางการแพทย์ในสถานพยาบาล และบริการที่ เกี่ยวข้องกับงานสนับสนุน 2) บริการที่เกี่ยวข้องกับการควบคุมการแพร่กระจายของเชื้อ โรคในสถานพยาบาล
2) มีการให้บริการสุขภาพ ระหว่างโรงพยาบาล	1) บริการทางการแพทย์ฉุกเฉินนอกสถานพยาบาล 2) บริการทางห้องปฏิบัติการ 3) บริการทางรังสีวิทยา 4) บริการโลหิต และคลังเลือด 5) บริการที่เกี่ยวข้องกับการควบคุมโรคติดต่อ
3) มีการให้บริการด้านยา เวชภัณฑ์ และเครื่องมือแพทย์	1) บริการที่เกี่ยวข้องกับการผลิตยา 2) บริการที่เกี่ยวข้องกับการผลิตเวชภัณฑ์ 3) บริการที่เกี่ยวข้องกับการผลิตเครื่องมือแพทย์ 4) บริการนำเข้า กระจายและจำหน่ายยา 5) บริการนำเข้า กระจายและจำหน่ายเวชภัณฑ์ 6) บริการนำเข้า กระจาย และจำหน่ายเครื่องมือแพทย์
4) มีการให้บริการตรวจวิเคราะห์ ทางแพทย์และรังสีวิทยา	1) บริการที่เกี่ยวข้องกับการตรวจวิเคราะห์ทางการแพทย์ 2) บริการทางรังสีวิทยา 3) บริการทางกัมมันตรังสี
5) มีการให้บริการข้อมูลสุขภาพ ดิจิทัล	1) บริการด้านการเงินการคลัง สุขภาพ 2) บริการคลังข้อมูลสุขภาพ 3) บริการที่เกี่ยวข้องกับระบบสุขภาพดิจิทัล

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 โรงพยาบาลของรัฐ และหน่วยงานสาธารณสุขถูกกำหนดให้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) จึงมีหน้าที่ต้องจัดทำนโยบายและแผนรักษาความมั่นคงปลอดภัยไซเบอร์ ประเมินความเสี่ยง กำหนด มาตรการป้องกัน จัดให้มีการตรวจสอบ ฝึกอบรม และซักซ้อมแผนรับมือเหตุการณ์ รวมถึงรายงานภัย คุกคามต่อหน่วยงานกำกับดูแลโดยไม่ชักช้า พร้อมให้ความร่วมมือในการตรวจสอบตามกฎหมาย โดย ระดับภัยคุกคามแบ่งเป็น ไม่ร้ายแรง ร้ายแรง และร้ายแรงมาก (วิกฤติ) ซึ่งมีผลต่อการกำหนด มาตรการและการใช้อำนาจของรัฐ หากไม่ปฏิบัติตามอาจมีโทษทั้งทางปกครองและทางอาญา ดังนั้น การที่โรงพยาบาลมีสถานะเป็น CII ทำให้การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์เป็นประเด็น

เชิงยุทธศาสตร์และธรรมาภิบาลองค์กร ไม่ใช่เพียงภารกิจของฝ่ายไอทีเท่านั้น การบูรณาการข้อกำหนดของกฎหมายดังกล่าวเข้ากับมาตรฐานสากล เช่น ISO/IEC 27001 และ NIST Cybersecurity Framework 2.0 จะช่วยให้โรงพยาบาลดำเนินการได้อย่างเป็นระบบ มีหลักฐานตรวจสอบได้ และลดความเสี่ยงต่อบทลงโทษทางกฎหมาย รวมทั้งรักษาความเชื่อมั่นของประชาชนในระยะยาว

2.3.2 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีผลบังคับใช้เต็มรูปแบบในเดือนมิถุนายน 2565 มีวัตถุประสงค์เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject) ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลอย่างปลอดภัย โดยแบ่งข้อมูลออกเป็น 2 ประเภท ได้แก่ (1) ข้อมูลส่วนบุคคลทั่วไป เช่น ชื่อ-นามสกุล ที่อยู่ เลขบัตรประชาชน และ (2) ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Personal Data) เช่น ข้อมูลสุขภาพ ข้อมูลชีวภาพ พันธุกรรม ความพิการ หรือความเชื่อทางศาสนา ซึ่ง “ข้อมูลสุขภาพ” ของผู้ป่วยที่โรงพยาบาลจัดเก็บถือเป็นข้อมูลอ่อนไหวและต้องได้รับการคุ้มครองเป็นพิเศษ ภายใต้หลักการบริหารความเสี่ยงตั้งแต่การระบุความเสี่ยง การป้องกัน การเฝ้าระวัง การตอบสนองเหตุการณ์ และการฟื้นฟูระบบ

กฎหมายกำหนดให้โรงพยาบาลในฐานะผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และ/หรือผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งด้านเทคนิคและกระบวนการ เช่น การกำหนดสิทธิการเข้าถึงตามหลัก Least Privilege/Need-to-Know การบริหารจัดการบัญชีผู้ใช้ (User Access Management) การพิสูจน์ตัวตนและกำหนดสิทธิ (Authentication & Authorization) การจัดทำบันทึกการใช้งาน (Audit Trails) และการป้องกันแบบหลายชั้น (Defense in Depth) รวมถึงการเข้ารหัสข้อมูลในระบบสำคัญ เช่น HIS และ EMR/EHR ตลอดจนต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) และดำเนินการตามสิทธิของเจ้าของข้อมูล เช่น สิทธิในการเข้าถึง แก้ไข ลบ หรือเพิกถอนความยินยอม อีกทั้งต้องแจ้งเหตุข้อมูลรั่วไหลภายในระยะเวลาที่กฎหมายกำหนด

หากไม่ปฏิบัติตาม อาจมีบทลงโทษ 3 ประเภท ได้แก่ โทษทางแพ่ง โทษทางอาญา และโทษทางปกครอง โดยมีค่าปรับทางปกครองสูงสุดถึง 5 ล้านบาท การปฏิบัติตาม PDPA จึงไม่ใช่เพียงภารกิจด้านกฎหมาย แต่เป็นรากฐานสำคัญของการพัฒนามาตรฐานความมั่นคงปลอดภัยไซเบอร์สำหรับโรงพยาบาล โดยควรบูรณาการกับมาตรฐานสากล เช่น ISO/IEC 27001 และแนวทางเฉพาะภาคสาธารณสุขอย่าง HAIT Plus เพื่อให้การคุ้มครองข้อมูลสุขภาพเป็นไปอย่างเป็นระบบ ตรวจสอบได้ และสอดคล้องทั้งกฎหมายไทยและหลักปฏิบัติสากล

2.3.3 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นกฎหมายหลักในการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์ของประเทศไทย มีบทบาทสำคัญต่อการดำเนินงานของโรงพยาบาลซึ่งมีการใช้ระบบสารสนเทศและจัดเก็บข้อมูลสุขภาพผู้ป่วยจำนวนมาก กฎหมายกำหนดความผิดเกี่ยวกับการเข้าถึงระบบหรือข้อมูลโดยมิชอบ การดักจับข้อมูล การทำให้ข้อมูลเสียหาย แก้ไข เปลี่ยนแปลง หรือรบกวนการทำงานของระบบคอมพิวเตอร์ รวมถึงกำหนดหน้าที่ของผู้ให้บริการในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log Files) ตามระยะเวลาที่กำหนด

สำหรับโรงพยาบาลซึ่งเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ด้านสาธารณสุข การปฏิบัติตามกฎหมายฉบับนี้จึงมีความจำเป็นอย่างยิ่ง โดยต้องจัดให้มีมาตรการป้องกันการเข้าถึงข้อมูลผู้ป่วยโดยมิชอบ เช่น การควบคุมสิทธิ์การเข้าถึง (Access Control) การเข้ารหัสข้อมูล (Encryption) และการจัดเก็บ Log Files อย่างครบถ้วนและตรวจสอบได้ หากเกิดเหตุข้อมูลรั่วไหลหรือระบบถูกโจมตี อาจเข้าข่ายความผิดตามกฎหมาย และก่อให้เกิดความรับผิดชอบทั้งทางแพ่งทางอาญา และทางปกครอง

ในการบริหารจัดการระบบสำคัญ เช่น HIS, EMR และฐานข้อมูลผู้ป่วย โรงพยาบาลจึงต้องคำนึงถึง (1) การป้องกันการเข้าถึงโดยมิชอบ (2) การจัดเก็บและบริหารจัดการ Log Files ตามที่กฎหมายกำหนด และ (3) การเตรียมความพร้อมด้านการตอบสนองต่อเหตุการณ์ (Incident Response) อย่างเป็นระบบ ทั้งนี้ควรบูรณาการการปฏิบัติตาม พ.ร.บ. คอมพิวเตอร์ ควบคู่กับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และมาตรฐานสากล เช่น ISO/IEC 27001 รวมถึงแนวทาง HAIT Plus เพื่อยกระดับความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลให้ครอบคลุมทั้งมิติด้านกฎหมาย มาตรฐาน และการบริหารจัดการความเสี่ยงอย่างครบวงจร.

2.3.4 ประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กระทรวงสาธารณสุข พ.ศ. 2565 เป็นกรอบนโยบายความมั่นคงปลอดภัยไซเบอร์ระดับกระทรวงที่ใช้กำกับหน่วยงานในสังกัดกระทรวงสาธารณสุขทั้งหมด โดยมุ่งเน้นการบริหารจัดการเชิงระบบอย่างบูรณาการ ครอบคลุมทั้งมิติบุคลากร (People) กระบวนการ (Process) และเทคโนโลยี (Technology) เพื่อปกป้องข้อมูลสุขภาพของประชาชนและลดความเสี่ยงจากภัยคุกคามไซเบอร์ ทั้งนี้ภาคสาธารณสุขถูกกำหนดให้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 จึงจำเป็นต้องมีมาตรการกลางที่ชัดเจนและเป็นมาตรฐานเดียวกันทั้งประเทศ

กรอบแนวทาง (Cybersecurity Policy Framework) ของประกาศดังกล่าวกำหนดมาตรการควบคุมที่ครอบคลุมด้านการกำกับดูแลและบริหารความเสี่ยง (Governance & Risk Management) การคุ้มครองข้อมูลส่วนบุคคลและข้อมูลสุขภาพ การควบคุมการเข้าถึงและการยืนยันตัวตน การเฝ้าระวังและตอบสนองเหตุการณ์ (Monitoring & Incident Response) และการบริหารความต่อเนื่องทางธุรกิจ (BCP/BCM) มาตรการสำคัญประกอบด้วย (1) การประเมินความเสี่ยงและการทดสอบเจาะระบบ (Risk Assessment & Penetration Testing) อย่างสม่ำเสมอ (2) การกำหนดนโยบายการใช้งานระบบสารสนเทศ เช่น นโยบายรหัสผ่านและการจัดชั้นความลับของข้อมูล (3) การสร้างความตระหนักรู้และฝึกอบรมบุคลากรต่อเนื่อง (4) การจัดทำและซักซ้อมแผนตอบสนองเหตุการณ์ (Incident Response Plan) และ (5) การบูรณาการมาตรฐานสากล เช่น ISO/IEC 27001 และ NIST Cybersecurity Framework ควบคู่กับกฎหมายไทย เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เป้าหมายของประกาศนโยบายนี้ คือ (1) สร้างมาตรฐานกลางด้านความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานสาธารณสุข (2) ลดความเสี่ยงจากการโจมตีและเหตุข้อมูลรั่วไหล (3) เสริมสร้างความเชื่อมั่นแก่ประชาชน ผู้ป่วย และหน่วยงานพันธมิตร และ (4) สนับสนุนการพัฒนาระบบสาธารณสุขดิจิทัล (Digital Health) ให้มีความปลอดภัย มั่นคง และยั่งยืนในระยะยาว.

เป้าหมายของการประกาศนโยบาย ได้แก่ 1) สร้างมาตรฐานกลางความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานด้านสาธารณสุข 2) ลดความเสี่ยงจากการโจมตีทางไซเบอร์และเหตุข้อมูลรั่วไหล 3) สร้างความเชื่อมั่นให้แก่ประชาชน ผู้ป่วย และหน่วยงานพันธมิตร และ 4) สนับสนุนการพัฒนาสาธารณสุขดิจิทัล (Digital Health) อย่างปลอดภัยและยั่งยืน

2.4 ทฤษฎีปัจจัยด้านการรับรู้และพฤติกรรมของบุคลากร

ทฤษฎีปัจจัยด้านการรับรู้และพฤติกรรมของบุคลากรมีรากฐานจากแนวคิดของ Icek Ajzen (1991) ซึ่งพัฒนา Theory of Planned Behavior (TPB) อธิบายว่าพฤติกรรมของบุคคลเกิดจาก “ความตั้งใจ” (Behavioral Intention) ที่ได้รับอิทธิพลจากการรับรู้ ทักษะ และแรงกดดันทางสังคม แนวคิดนี้สามารถประยุกต์ใช้กับบริบทความมั่นคงปลอดภัยไซเบอร์ในโรงพยาบาลได้อย่างชัดเจน

2.4.1 การรับรู้ (Perception) คือ กระบวนการที่บุคลากรตีความข้อมูล ประสบการณ์ และสิ่งเร้า แล้วแปลงเป็นความเข้าใจหรือความเชื่อ ซึ่งมีผลโดยตรงต่อทัศนคติและความตั้งใจในการปฏิบัติตามมาตรการความมั่นคงปลอดภัย ปัจจัยสำคัญ ได้แก่

2.4.1.1 ความรู้และประสบการณ์ (Knowledge & Experience) บุคลากรที่เคยเผชิญเหตุข้อมูลรั่วไหลหรือการโจมตีทางไซเบอร์ จะตระหนักถึงความสำคัญของมาตรการมากขึ้น

2.4.1.2 การรับรู้ประโยชน์ (Perceived Usefulness) หากมองเห็นว่ามาตรฐานช่วยปกป้องข้อมูลผู้ป่วย ลดความเสี่ยง และเพิ่มความเชื่อมั่น ก็มีแนวโน้มยอมรับและปฏิบัติตาม

2.4.1.3 การรับรู้ความง่ายในการใช้งาน (Perceived Ease of Use) หากมาตรการหรือระบบไม่ซับซ้อน ใช้งานสะดวก จะช่วยสร้างทัศนคติที่ดีต่อการปฏิบัติ

2.4.1.4 การรับรู้ความเสี่ยง (Perceived Risk) การตระหนักถึงผลกระทบจากการไม่ปฏิบัติตาม เช่น การถูกโจมตีหรือข้อมูลรั่วไหล จะกระตุ้นให้เกิดพฤติกรรมป้องกัน

2.4.2 พฤติกรรม (Behavior) คือ การแสดงออกที่เกิดจากการรับรู้ ทักษะ และแรงกดดันทางสังคม ในงานด้านความมั่นคงปลอดภัยไซเบอร์ พฤติกรรมของบุคลากรมีผลโดยตรงต่อระดับความปลอดภัยของระบบสารสนเทศ ตัวอย่างพฤติกรรมที่พึงประสงค์ ได้แก่

2.4.2.1 การตั้งรหัสผ่านที่มีความแข็งแรง

2.4.2.2 การปฏิบัติตามมาตรฐาน เช่น ISO/IEC 27001 และแนวทาง HAIT Plus

2.4.2.3 การรายงานเหตุการณ์ผิดปกติหรือภัยคุกคามโดยทันที

2.4.2.4 การไม่เปิดเผยรหัสผ่านหรือข้อมูลผู้ป่วยแก่บุคคลที่ไม่เกี่ยวข้อง

2.4.3 ปัจจัยที่มีอิทธิพลต่อพฤติกรรม ได้แก่

2.4.3.1 ทัศนคติ (Attitude): หากเชื่อว่ามาตรการช่วยเพิ่มความปลอดภัยจริง จะมีแนวโน้มปฏิบัติตาม

2.4.3.2 บรรทัดฐานทางสังคม (Subjective Norms): การเน้นย้ำจากผู้บริหารหรือเพื่อนร่วมงาน ส่งผลให้เกิดแรงผลักดันเชิงบวก

2.4.3.3 การรับรู้ความสามารถของตนเอง (Self-Efficacy / Perceived Behavioral Control): ความมั่นใจว่ามีความรู้และทักษะเพียงพอในการปฏิบัติตามมาตรการ

โดยสรุป ทฤษฎีของ Ajzen ชี้ให้เห็นว่า การยกระดับความมั่นคงปลอดภัยไซเบอร์ในโรงพยาบาลไม่อาจพึ่งพาเทคโนโลยีเพียงอย่างเดียว แต่ต้องพัฒนา “การรับรู้ ทัศนคติ และความเชื่อมั่น” ของบุคลากรควบคู่กัน เพื่อให้เกิดพฤติกรรมด้านความปลอดภัยที่ยั่งยืนในองค์กร.

2.5 ทฤษฎีที่เกี่ยวข้องกับการยอมรับเทคโนโลยีสารสนเทศ

ทฤษฎีการยอมรับเทคโนโลยี (TAM) พัฒนาโดย Fred Davis (1989) เพื่ออธิบายเหตุผลที่บุคคลตัดสินใจยอมรับหรือปฏิเสธการใช้เทคโนโลยี โดยเน้นปัจจัยด้านการรับรู้ของผู้ใช้เป็นสำคัญ แบบจำลองนี้เสนอว่า “การรับรู้” จะส่งผลต่อ “ทัศนคติ” และนำไปสู่ “ความตั้งใจ” และ “การใช้งานจริง” ตามลำดับ

2.5.1 องค์ประกอบสำคัญของ TAM ได้แก่

2.5.1.1 การรับรู้ประโยชน์ (Perceived Usefulness: PU) บุคลากรเชื่อว่าการใช้มาตรฐานหรือระบบจะช่วยเพิ่มประสิทธิภาพการทำงาน ลดความเสี่ยง และสร้างความน่าเชื่อถือ เช่น การนำมาตรฐาน ISO/IEC 27001:2022 และแนวทาง HAIT Plus มาใช้ อาจช่วยลดโอกาสข้อมูลรั่วไหล เสริมความเชื่อมั่นของผู้ป่วย และยกระดับภาพลักษณ์องค์กร

2.5.1.2 การรับรู้ความง่ายในการใช้งาน (Perceived Ease of Use: PEOU) บุคลากรเชื่อว่าการปฏิบัติตามมาตรฐานหรือการใช้ระบบไม่ซับซ้อน สามารถเรียนรู้และใช้งานได้ง่าย เช่น มีนโยบาย (Policy) และขั้นตอนปฏิบัติ (Procedure) ชัดเจน มีการอบรมและเครื่องมือสนับสนุนที่เหมาะสม

2.5.1.3 ทัศนคติต่อการใช้งาน (Attitude Toward Using: ATU) หากบุคลากรรับรู้ว่ามีประโยชน์และใช้งานง่าย จะก่อให้เกิดทัศนคติในเชิงบวกต่อการนำมาตรฐานหรือเทคโนโลยีมาใช้

2.5.1.4 ความตั้งใจที่จะใช้ (Behavioral Intention to Use) ทัศนคติที่ดีจะนำไปสู่ความตั้งใจในการปฏิบัติตามมาตรการด้านความมั่นคงปลอดภัยไซเบอร์

2.5.1.5 การใช้งานจริง (Actual System Use: ASU) ความตั้งใจที่เข้มแข็งจะส่งผลให้เกิดพฤติกรรมการใช้งานจริงอย่างต่อเนื่อง

ต่อมาได้มีการพัฒนาแบบจำลองเพิ่มเติม เช่น TAM2 และ TAM3 ซึ่งเพิ่มปัจจัยด้านอิทธิพลทางสังคม ประสบการณ์ และเงื่อนไขสนับสนุน เพื่ออธิบายการยอมรับเทคโนโลยีในบริบทองค์กรได้ครอบคลุมยิ่งขึ้น

2.5.2 ทฤษฎีพฤติกรรมตามแผน (Theory of Planned Behavior: TPB)

ทฤษฎีพฤติกรรมตามแผน (TPB) พัฒนาโดย Icek Ajzen (1991) อธิบายว่าพฤติกรรมของบุคคลไม่ได้เกิดขึ้นโดยบังเอิญ แต่เกิดจาก “ความตั้งใจ” (Intention) ซึ่งได้รับอิทธิพลจาก 3 ปัจจัยหลัก ได้แก่

2.5.2.1 ทัศนคติต่อพฤติกรรม (Attitude Toward Behavior) ความเชื่อว่าการกระทำนั้นก่อให้เกิดผลดีหรือผลเสีย หากบุคลากรเชื่อว่าการปฏิบัติตามมาตรฐานไซเบอร์ช่วยปกป้องข้อมูลผู้ป่วยและลดความเสี่ยง ก็จะมีแนวโน้มปฏิบัติตาม

2.5.2.2 บรรทัดฐานเชิงอัตวิสัย (Subjective Norms) การรับรู้แรงกดดันหรือความคาดหวังจากผู้บริหาร เพื่อนร่วมงาน หรือองค์กร หากผู้บริหารให้ความสำคัญกับมาตรการไซเบอร์อย่างจริงจัง บุคลากรก็จะรู้สึกว่าการปฏิบัติตาม

2.5.2.3 การรับรู้ความสามารถในการควบคุมพฤติกรรม (Perceived Behavioral Control: PBC) ความเชื่อว่าตนเองมีความรู้ ทักษะ และทรัพยากรเพียงพอ หากมีการอบรมคู่มือ และระบบสนับสนุนที่เหมาะสม บุคลากรจะมั่นใจว่าสามารถปฏิบัติตามมาตรฐานได้จริง

TAM มุ่งเน้นการอธิบาย “การยอมรับเทคโนโลยี” ผ่านการรับรู้ประโยชน์และความง่ายในการใช้งาน ขณะที่ TPB อธิบาย “พฤติกรรม” ผ่านทัศนคติ บรรทัดฐานทางสังคม และการรับรู้ความสามารถควบคุมตนเอง เมื่อนำมาประยุกต์ใช้ในบริบทโรงพยาบาล จะช่วยอธิบายได้ว่า การยกระดับมาตรฐานความมั่นคงปลอดภัยไซเบอร์ให้ประสบความสำเร็จ ไม่ได้ขึ้นอยู่กับเทคโนโลยีเพียงอย่างเดียว แต่ต้องสร้างการรับรู้ที่ถูกต้อง ทัศนคติที่ดี และสภาพแวดล้อมองค์กรที่สนับสนุนการปฏิบัติอย่างต่อเนื่องและยั่งยืน

2.6 งานวิจัยที่เกี่ยวข้อง

สำหรับงานวิจัยในปัจจุบันที่เกี่ยวข้องกับการวิเคราะห์ปัจจัยการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล มีงานวิจัยที่เกี่ยวข้องดังนี้

Hair, J. F. และคณะ (2019) ได้ทำการศึกษาวิจัยและเรียบเรียงองค์ความรู้ด้านการวิเคราะห์ข้อมูลพหุคูณในหนังสือ *Multivariate Data Analysis* โดยมุ่งเน้นการอธิบายหลักการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) และการประเมินความเที่ยงตรงของโครงสร้าง ผลการศึกษาสรุปว่า การวิเคราะห์ EFA ควรพิจารณาค่า factor loading ไม่ต่ำกว่า 0.50 การตรวจสอบค่า KMO และ Bartlett's Test เพื่อยืนยันความเหมาะสมของข้อมูล รวมถึงการประเมินความสอดคล้องเชิงทฤษฎีควบคู่กับผลทางสถิติ เพื่อให้ได้โครงสร้างที่มีความเที่ยงตรงเชิงโครงสร้าง (construct validity)

Kaiser, H. F. (1974) ได้ทำการศึกษาวิจัยเกี่ยวกับดัชนีวัดความเหมาะสมของข้อมูลสำหรับการวิเคราะห์องค์ประกอบ และเสนอค่า Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy ผลการวิจัยพบว่า ค่า KMO ที่มีค่ามากกว่า 0.50 ถือว่ายอมรับได้ และหากมีค่ามากกว่า .80 จะถือว่ามีความเหมาะสมในระดับดีมากสำหรับการวิเคราะห์องค์ประกอบ

Tabachnick, B. G. และ Fidell, L. S. (2019) ได้ศึกษาวิธีการใช้สถิติพหุคูณทางพฤติกรรมศาสตร์ โดยให้แนวทางเกี่ยวกับเกณฑ์การพิจารณาค่าองค์ประกอบและการหมุนแกน (rotation) ผลการศึกษาชี้ให้เห็นว่า การหมุนแกนแบบ Varimax ช่วยเพิ่มความชัดเจนของโครงสร้างองค์ประกอบ และควรพิจารณาค่า communalities และ cross-loading อย่างรอบคอบก่อนตัดสินใจคงไว้หรือข้อคำถาม

Davis, F. D. (1989) ได้ทำการศึกษาวิจัยเรื่องการพัฒนาแบบจำลองการยอมรับเทคโนโลยี (Technology Acceptance Model: TAM) เพื่ออธิบายปัจจัยที่มีอิทธิพลต่อความตั้งใจในการใช้ระบบสารสนเทศ ผลการศึกษาพบว่า การรับรู้ประโยชน์ (Perceived Usefulness: PU) และการรับรู้

ความง่ายในการใช้งาน (Perceived Ease of Use: PEOU) มีอิทธิพลเชิงบวกต่อทัศนคติและความตั้งใจในการใช้เทคโนโลยีอย่างมีนัยสำคัญทางสถิติ

Venkatesh, V. และคณะ (2003) ได้ทำการศึกษาวิจัยเรื่องการบูรณาการทฤษฎีการยอมรับเทคโนโลยีหลายกรอบแนวคิด และพัฒนาแบบจำลอง UTAUT (Unified Theory of Acceptance and Use of Technology) ผลการศึกษาพบว่า ปัจจัยด้านความคาดหวังด้านประสิทธิภาพ (Performance Expectancy) ความคาดหวังด้านความพยายาม (Effort Expectancy) อิทธิพลทางสังคม (Social Influence) และเงื่อนไขสนับสนุน (Facilitating Conditions) มีอิทธิพลต่อความตั้งใจและพฤติกรรมการใช้เทคโนโลยี โดยมีตัวแปรกำกับ ได้แก่ เพศ อายุ ประสบการณ์ และความสมัครใจในการใช้

จากทฤษฎีและงานวิจัยที่ได้ศึกษาข้างต้น สรุปได้ ดังนี้ โรงพยาบาลเป็นหน่วยงานที่ต้องรักษาทั้ง ความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูล ควบคู่กับความต่อเนื่องของบริการรักษาพยาบาล ซึ่งเชื่อมโยงโดยตรงกับความปลอดภัยของผู้ป่วย

ในด้านกฎหมาย งานวิจัยชี้ให้เห็นความสำคัญของ พ.ร.บ. Cybersecurity, PDPA, พ.ร.บ. คอมพิวเตอร์ และนโยบายกระทรวงสาธารณสุข ซึ่งทำให้ความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลเป็นทั้งภารกิจด้านเทคนิค กฎหมาย และธรรมาภิบาลองค์กร

ด้านทฤษฎี มีการกล่าวถึงการใช้ทฤษฎีพฤติกรรมตามแผน (Theory of Planned Behavior: TPB) และแบบจำลองการยอมรับเทคโนโลยีสารสนเทศ (Technology Acceptance Model: TAM) อธิบายว่า การยอมรับมาตรการไซเบอร์ของบุคลากรขึ้นอยู่กับความรู้ประโยชน์ ความง่ายในการใช้งาน ทัศนคติ บรรทัดฐานทางสังคม และความเชื่อมั่นในความสามารถของตนเอง

ข้อค้นพบหลักคือ การยกระดับไซเบอร์ในโรงพยาบาลไม่อาจพึ่งเทคโนโลยีเพียงอย่างเดียว แต่ต้องพัฒนา People, Process, Technology และ Governance ไปพร้อมกัน นอกจากนี้วรรณกรรมที่บทวนยังสนับสนุนความแข็งแกร่งของระเบียบวิธีวิจัย โดยอ้างอิงแนวคิดด้าน EFA, KMO, Bartlett's Test และ Construct Validity เพื่อรองรับการพัฒนาเครื่องมือวิจัยอย่างมีความน่าเชื่อถือ

ในเชิงวิชาการ บทนี้มีคุณค่าเพราะสร้างกรอบบูรณาการระหว่าง มาตรฐาน กฎหมาย และพฤติกรรมมนุษย์ ซึ่งช่วยขยายการศึกษาด้านไซเบอร์จากมุมเทคนิคสู่มุมการจัดการและพฤติกรรมองค์กร

ในเชิงปฏิบัติ แต่ละทฤษฎี บทนี้มีความสำคัญต่อโรงพยาบาลอย่างมาก เพราะช่วยชี้แนวทางในการออกแบบนโยบาย มาตรการควบคุม การอบรมบุคลากร และระบบตอบสนองเหตุการณ์ให้สอดคล้องกับความเสี่ยงจริงของภาคสาธารณสุข

สรุปได้ว่า ทฤษฎีและงานวิจัยที่ได้ศึกษา มีความโดดเด่นตรงการมองความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลแบบองค์รวม ไม่แยกส่วน และสามารถต่อยอดได้ทั้งในเชิงวิชาการ การประเมินความพร้อม และการพัฒนามาตรฐานความปลอดภัยไซเบอร์ของโรงพยาบาลไทยอย่างเป็นรูปธรรม

บทที่ 3

วิธีดำเนินการวิจัย

การวิจัย เรื่อง แนวทางพัฒนาการออกแบบเทคโนโลยีความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล เพื่อสอดคล้องกับมาตรฐาน HAIT Plus และ ISO 27001 ผู้วิจัยใช้วิธีการวิจัยเชิงปริมาณ ดังนี้

- 3.1 กำหนดปัญหาและวัตถุประสงค์การวิจัย
- 3.2 ประชากรและกลุ่มตัวอย่าง
- 3.4 เครื่องมือที่ใช้ในการวิจัย
- 3.5 วิธีดำเนินงานวิจัยและการเก็บรวบรวมข้อมูล
- 3.6 วิธีการวิเคราะห์ข้อมูล

3.1 กำหนดปัญหาและวัตถุประสงค์การวิจัย

ปัจจุบันภัยคุกคามทางไซเบอร์ถือเป็นความเสี่ยงระดับโลกที่ก่อให้เกิดความเสียหายทั้งต่อบุคคล หน่วยงาน และระดับประเทศ โดยจากรายงาน The Global Risk Report 2025 ของ World Economic Forum (2024) พบว่า ความไม่มั่นคงทางไซเบอร์ถูกจัดให้เป็นหนึ่งใน 10 อันดับความเสี่ยงสำคัญ ที่อาจนำไปสู่วิกฤติในระดับโลก ทั้งในช่วง 2 ปีข้างหน้า (อันดับ 4) และ อีก 10 ปีข้างหน้า (อันดับ 10) สะท้อนถึงแนวโน้มความรุนแรงที่ทวีความสำคัญมากยิ่งขึ้น

สำหรับภาคสาธารณสุข งานวิจัยของ Journal of The American Medical Association (2023) ระบุว่า การโจมตีไซเบอร์ต่อระบบสาธารณสุขมีค่าเฉลี่ยสูงถึง 1,684 ครั้งต่อสัปดาห์ในไตรมาส 1 ปี 2566 เพิ่มขึ้นกว่า 22% จากปีก่อนหน้า ในประเทศไทย สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) รายงานว่า หน่วยงานสาธารณสุขถูกโจมตีเป็น อันดับ 8 ของประเทศ จำนวน 75 ครั้ง ในปี พ.ศ. 2567

โรงพยาบาลและสถานพยาบาลในไทยมีจำนวนมากกว่า 11,940 แห่ง ครอบคลุมตั้งแต่โรงพยาบาลศูนย์ โรงพยาบาลทั่วไป จนถึงโรงพยาบาลชุมชน (สำนักงานสถิติแห่งชาติ, 2567) โดยเป็นหน่วยงานที่มีภารกิจรับผิดชอบต่อชีวิตโดยตรงและเก็บรักษาข้อมูลสำคัญ เช่น ประวัติการรักษา ข้อมูลส่วนบุคคลทั่วไป ข้อมูลอ่อนไหว ตลอดจนข้อมูลของบุคคลสำคัญ ซึ่งหากเกิดเหตุการณ์ข้อมูลรั่วไหลหรือถูกโจมตีไซเบอร์ จะส่งผลกระทบอย่างร้ายแรงทั้งต่อระบบบริการสุขภาพและความเชื่อมั่นของประชาชน

แม้กระทรวงสาธารณสุขได้ประกาศ นโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ พ.ศ. 2565 แต่จากรายงานของ สำนักงานสถิติแห่งชาติและกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ. 2567) ยังพบว่าสถานพยาบาลติดอันดับกลุ่มหน่วยงานที่ถูกโจมตีไซเบอร์อย่างต่อเนื่อง รวมถึงมีกรณีข้อมูลส่วนบุคคลรั่วไหลไปยัง Dark Web ที่สร้างความกังวลต่อความปลอดภัยของข้อมูลผู้ป่วยและระบบบริการ

เพื่อลดความเสี่ยงดังกล่าว หน่วยงานสาธารณสุขจำเป็นต้องบูรณาการมาตรการป้องกันภัยไซเบอร์ โดยครอบคลุมทั้ง ด้านบุคลากร กระบวนการ และเทคโนโลยี ผ่านการนำมาตรฐานสากล เช่น

HAIT Plus, ISO/IEC 27001:2022 มาใช้ รวมถึงการทำ Vulnerability Assessment, Penetration Testing และการพัฒนาศักยภาพบุคลากร เพื่อยกระดับความมั่นคงปลอดภัยของระบบสารสนเทศ ด้านสาธารณสุขอย่างมีประสิทธิภาพ

3.2 ประชากรและกลุ่มตัวอย่าง

การกำหนดประชากรและกลุ่มตัวอย่างในการวิจัยครั้งนี้ แบ่งออกเป็น 2 ส่วน ได้แก่ การวิจัยเชิงปริมาณ (Quantitative Research) และการวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีรายละเอียดดังต่อไปนี้

3.2.1 การวิจัยเชิงปริมาณ (Quantitative Research)

3.2.1.1 ประชากร (Population) ที่ใช้ในการวิจัยเชิงปริมาณ ได้แก่ บุคลากรที่ปฏิบัติงานใน โรงพยาบาลธรรมศาสตร์เฉลิมพระเกียรติ ซึ่งประกอบด้วยบุคลากรสายการแพทย์ พยาบาล บุคลากรด้านเทคโนโลยีสารสนเทศ บุคลากรฝ่ายสนับสนุน และผู้บริหารที่มีส่วนเกี่ยวข้องกับการใช้งานระบบสารสนเทศและการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของโรงพยาบาล

3.2.1.2 การกำหนดขนาดกลุ่มตัวอย่าง (Sample Size) พิจารณาตามหลักการกำหนดขนาดตัวอย่างสำหรับการวิเคราะห์โมเดลสมการโครงสร้าง (Structural Equation Modeling: SEM) โดยอ้างอิงแนวคิดของ Hair, J. F. และคณะ (2019) ที่เสนอให้มีจำนวนตัวอย่างอย่างน้อย 5–10 เท่าของจำนวนตัวชี้วัดทั้งหมดในแบบสอบถาม หรือไม่น้อยกว่า 200 ตัวอย่าง เพื่อให้เพียงพอต่อการวิเคราะห์ทางสถิติขั้นสูง

3.2.1.3 วิธีการสุ่มตัวอย่าง ใช้วิธีการสุ่มแบบแบ่งชั้น (Stratified Sampling) ตามกลุ่มสายงาน เพื่อให้ได้กลุ่มตัวอย่างที่ครอบคลุมบทบาทหน้าที่ที่หลากหลายภายในองค์กร และลดความเอนเอียงของข้อมูล

3.2.1.4 เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล ได้แก่ แบบสอบถามมาตราส่วนประมาณค่า 5 ระดับ (5-Point Likert Scale) ซึ่งผ่านการตรวจสอบความตรงเชิงเนื้อหา (Content Validity) โดยผู้ทรงคุณวุฒิ และทดสอบความเชื่อมั่น (Reliability) ด้วยค่าสัมประสิทธิ์แอลฟาของครอนบาค (Cronbach's Alpha) ตามแนวทางของ Cronbach, Lee J. (1951)

3.2.2 การวิจัยเชิงคุณภาพ (Qualitative Research) การวิจัยเชิงคุณภาพในครั้งนี้มีวัตถุประสงค์เพื่อสนับสนุนและอธิบายผลการวิจัยเชิงปริมาณ โดยใช้แนวทางดังต่อไปนี้

3.2.2.1 วิจัยเชิงเอกสาร (Document Research) จากเอกสารที่เกี่ยวข้องกับนโยบายคุณภาพ นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ และเอกสารอื่นที่เกี่ยวข้อง

โดยสรุป การกำหนดประชากรและกลุ่มตัวอย่างในงานวิจัยครั้งนี้มีความครอบคลุมทั้งมิติข้อมูลเชิงปริมาณและเชิงคุณภาพ เพื่อให้สามารถอธิบายปรากฏการณ์ด้านการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างรอบด้าน และเพิ่มความน่าเชื่อถือของผลการวิจัยตามหลักระเบียบวิธีวิจัยระดับบัณฑิตศึกษา

3.3 เครื่องมือที่ใช้ในการวิจัย

การวิจัยครั้งนี้ใช้เครื่องมือในการเก็บรวบรวมข้อมูลทั้งเชิงปริมาณและเชิงคุณภาพ โดยพัฒนาให้สอดคล้องกับกรอบแนวคิดการวิจัย และผ่านกระบวนการตรวจสอบคุณภาพเครื่องมือตามหลักวิชาการ ดังรายละเอียดต่อไปนี้

3.3.1 การวิจัยเชิงปริมาณ (Quantitative Research) โดยใช้ระเบียบวิธีวิจัยเชิงสำรวจ (Survey) เครื่องมือในการวิจัย ได้แก่ แบบสอบถาม (Questionnaire) ทั้งแบบออนไลน์ และรูปแบบเอกสาร

3.3.1.1 วัดระดับการรับรู้มาตรฐาน ส่วนนี้พัฒนาข้อคำถามเพื่อวัดระดับการรับรู้ของบุคลากรเกี่ยวกับมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับบริบทโรงพยาบาล ได้แก่

3.3.1.1.1 มาตรฐาน HAIT Plus ภายใต้การกำกับของ สถาบันรับรองคุณภาพสถานพยาบาล (องค์การมหาชน)

3.3.1.1.2 มาตรฐาน International Organization for Standardization ในส่วนของ ISO/IEC 27001 ด้านระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS)

ลักษณะข้อคำถามเป็นมาตราส่วนประมาณค่า 5 ระดับ (5-Point Likert Scale) ตั้งแต่ระดับเห็นด้วยอย่างยิ่ง ถึงไม่เห็นด้วยอย่างยิ่ง โดยครอบคลุมมิติสำคัญ

3.3.1.2 ประเมินปัจจัยสนับสนุน ส่วนนี้มุ่งวัดปัจจัยสนับสนุนที่ส่งผลต่อการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล ประกอบด้วยตัวแปรแฝง (Latent Variables) ที่สำคัญ ได้แก่

3.3.1.2.1 ด้านงบประมาณ (Budget Support)

3.3.1.2.2 ด้านการฝึกอบรมและพัฒนาบุคลากร (Training and Development)

3.3.1.2.3 ด้านทีมงานและโครงสร้างการบริหาร (Team and Governance Structure)

การพัฒนาข้อคำถามอ้างอิงแนวคิดการสนับสนุนองค์กร (Organizational Support) และหลักการบริหารความมั่นคงปลอดภัยสารสนเทศ โดยข้อคำถามผ่านการตรวจสอบความตรงเชิงเนื้อหา (Content Validity) จากผู้ทรงคุณวุฒิ และทดสอบความเชื่อมั่นด้วยค่าสัมประสิทธิ์แอลฟาของครอนบาค (Cronbach's Alpha) ตามแนวคิดของ Cronbach, Lee J. (1951) โดยกำหนดเกณฑ์ค่าความเชื่อมั่นไม่ต่ำกว่า 0.70

3.3.1.3 วิเคราะห์ความสัมพันธ์ด้วยสถิติ Path Analysis ภายหลังจากตรวจสอบคุณภาพข้อมูลเบื้องต้น ได้แก่ ความครบถ้วนของข้อมูล การตรวจสอบค่าผิดปกติ (Outliers) และการทดสอบสมมติฐานเบื้องต้นของข้อมูลแล้ว ผู้วิจัยดำเนินการวิเคราะห์ความสัมพันธ์เชิงสาเหตุระหว่างตัวแปรด้วยสถิติ Path Analysis ภายใตกรอบแนวคิดของการวิเคราะห์โมเดลสมการโครงสร้าง (Structural Equation Modeling: SEM)

แนวทางการวิเคราะห์อ้างอิงหลักการของ Hair, J. F. และคณะ (2019) โดยพิจารณา ค่าสัมประสิทธิ์เส้นทาง (Path Coefficient: β), ค่า t-value, ค่า p-value และค่าสัมประสิทธิ์การ อธิบายความแปรปรวน (R^2) เพื่อประเมินพลังการอธิบายของแบบจำลอง

3.3.2 การวิจัยเชิงคุณภาพ (Qualitative Research) ดังนี้

วิจัยเชิงเอกสาร (Document Research) การวิจัยเชิงคุณภาพในครั้งนี้ใช้วิธีการวิจัยเชิง เอกสาร (Documentary Research) โดยศึกษาจากเอกสารที่เกี่ยวข้องกับการบริหารจัดการความ มั่นคงปลอดภัยสารสนเทศของโรงพยาบาล ได้แก่

- 3.3.2.1 นโยบายคุณภาพองค์กร
- 3.3.2.2 นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
- 3.3.2.3 คู่มือการปฏิบัติงานด้านความปลอดภัยสารสนเทศ
- 3.3.2.4 รายงานการตรวจประเมินภายในและภายนอก
- 3.3.2.5 เอกสารอ้างอิงมาตรฐานที่เกี่ยวข้อง เช่น ISO/IEC 27001 และ HAIT Plus

3.4 วิธีดำเนินการวิจัยและการเก็บรวบรวมข้อมูล

การดำเนินการวิจัยครั้งนี้เป็นการวิจัยแบบผสมผสาน (Mixed Methods Research) โดยมุ่ง ศึกษาเชิงปริมาณควบคู่กับการวิเคราะห์เชิงคุณภาพ เพื่อให้ได้ผลการวิจัยที่มีความครอบคลุมและรอบ ด้าน ผู้วิจัยได้กำหนดขั้นตอนการดำเนินการวิจัยและการเก็บรวบรวมข้อมูลอย่างเป็นระบบ ดังต่อไปนี้

3.4.1 ขั้นตอนที่ 1 การออกแบบแบบสอบถามและการทดสอบคุณภาพเครื่องมือ ผู้วิจัย ดำเนินการออกแบบแบบสอบถามตามกรอบแนวคิดการวิจัย โดยอ้างอิงแนวคิดด้านการบริหารจัดการ ความมั่นคงปลอดภัยสารสนเทศ และข้อกำหนดของมาตรฐานที่เกี่ยวข้อง

3.4.2 ขั้นตอนที่ 2 การเก็บรวบรวมข้อมูล ภายหลังการปรับปรุงแบบสอบถามให้มีความ สมบูรณ์ ผู้วิจัยดำเนินการเก็บรวบรวมข้อมูลจากบุคลากรของ โรงพยาบาลธรรมศาสตร์เฉลิมพระ เกียรติ โดยใช้ทั้งแบบสอบถามออนไลน์และแบบเอกสาร ผู้วิจัยชี้แจงวัตถุประสงค์ของการวิจัย การ รักษาความลับของข้อมูล และขอความยินยอมก่อนการตอบแบบสอบถาม ทั้งนี้ การเก็บรวบรวม ข้อมูลดำเนินการภายในระยะเวลาที่กำหนด และตรวจสอบความครบถ้วนของแบบสอบถามก่อนนำไป วิเคราะห์

3.4.3 ขั้นตอนที่ 3 การวิเคราะห์ข้อมูลทางสถิติ ข้อมูลที่ได้รับนำมาตรวจสอบความสมบูรณ์ และคัดกรองข้อมูลที่ไม่สมบูรณ์ออก จากนั้นดำเนินการวิเคราะห์ข้อมูลด้วยโปรแกรมสำเร็จรูปทาง สถิติ โดยแบ่งการวิเคราะห์ออกเป็น 3 ระดับ การวิเคราะห์สถิติเชิงพรรณนา (Descriptive Statistics) การทดสอบคุณภาพโมเดลการวัด (Measurement Model) การวิเคราะห์ความสัมพันธ์เชิงสาเหตุ ด้วย Path Analysis

3.4.4 ขั้นตอนที่ 4 การสังเคราะห์ผลการตอบแบบสอบถาม ภายหลังการวิเคราะห์เชิงสถิติ ผู้วิจัยดำเนินการสังเคราะห์ผลการวิจัย โดยเชื่อมโยงผลการวิเคราะห์เชิงปริมาณกับข้อมูลจากการวิจัย เชิงเอกสาร เพื่ออธิบายบริบทขององค์กร ปัจจัยเชิงนโยบาย และข้อกำหนดของมาตรฐานที่เกี่ยวข้อง การสังเคราะห์ผลเน้นการวิเคราะห์เชิงเหตุผล (Analytical Interpretation) เพื่ออธิบายกลไก ความสัมพันธ์ของตัวแปร และตรวจสอบความสอดคล้องกับทฤษฎีและงานวิจัยที่ผ่านมา

3.4.5 ขั้นตอนที่ 5 การสรุปและอภิปรายผล โดยการสรุปผลการศึกษาวิจัย และข้อเสนอแนะในการวิจัยครั้งต่อไป รวมถึงการนำไปใช้

3.5 วิธีการวิเคราะห์ข้อมูล

ภายหลังจากรวบรวมข้อมูลจากแบบสอบถามเรื่อง “ปัจจัยการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล” เรียบร้อยแล้ว ผู้วิจัยจะดำเนินการประมวลผลและวิเคราะห์ข้อมูลด้วยโปรแกรมคอมพิวเตอร์สำเร็จรูป โดยแบ่งการวิเคราะห์ออกเป็น 2 ส่วนหลัก ได้แก่ สถิติเชิงพรรณนา และสถิติเชิงอนุมาน ดังนี้

3.5.1 สถิติเชิงพรรณนา (Descriptive Statistics)

สถิติเชิงพรรณนาจะถูกนำมาใช้เพื่ออธิบายและสรุปภาพรวมข้อมูลพื้นฐานของกลุ่มตัวอย่าง รวมถึงลักษณะการตอบแบบสอบถามในเบื้องต้น ประกอบด้วย

3.5.1.1 การวิเคราะห์ข้อมูลส่วนบุคคล ใช้สถิติ ค่าความถี่ (Frequency) และ ค่าร้อยละ (Percentage) เพื่ออธิบายลักษณะทางประชากรศาสตร์ของกลุ่มตัวอย่าง เช่น เพศ อายุ ระดับการศึกษา และตำแหน่งงาน

3.5.1.2 การวิเคราะห์ข้อมูลตัวแปรหลัก: ใช้สถิติ ค่าเฉลี่ย (Mean) และ ค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) เพื่ออธิบายระดับการรับรู้และความคิดเห็นของกลุ่มตัวอย่างที่มีต่อตัวแปรแต่ละตัวในกรอบแนวคิดการวิจัย ซึ่งจะช่วยให้เห็นภาพรวมแนวโน้มการตอบของผู้เข้าร่วมวิจัย

3.5.2 สถิติเชิงอนุมาน (Inferential Statistics)

สถิติเชิงอนุมานใช้เพื่อทดสอบสมมติฐานการวิจัยและตรวจสอบความสัมพันธ์ระหว่างตัวแปรตามกรอบแนวคิดที่กำหนดไว้ โดยประกอบด้วย

3.5.2.1 การวิเคราะห์ความสัมพันธ์ (Correlation Analysis) ใช้ค่าสัมประสิทธิ์สหสัมพันธ์เพียร์สัน (Pearson's Correlation Coefficient) เพื่อวิเคราะห์ทิศทางและระดับความสัมพันธ์ระหว่างตัวแปรอิสระและตัวแปรตาม ทั้งนี้เพื่อพิจารณาความสัมพันธ์เบื้องต้นก่อนการวิเคราะห์เชิงสาเหตุในขั้นถัดไป

3.5.2.2 การวิเคราะห์การถดถอยพหุคูณ (Multiple Regression Analysis) ใช้เพื่อวิเคราะห์อิทธิพลของตัวแปรอิสระหลายตัวที่มีต่อตัวแปรตาม พร้อมทั้งประเมินค่าสัมประสิทธิ์การถดถอย (Regression Coefficient: β) ค่าสัมประสิทธิ์การกำหนด (R^2) และระดับนัยสำคัญทางสถิติ (p-value) เพื่อพิจารณาว่าปัจจัยใดมีอิทธิพลอย่างมีนัยสำคัญต่อการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ของโรงพยาบาล

การวิเคราะห์ทั้งสองระดับดังกล่าวช่วยให้การแปลผลข้อมูลมีความครบถ้วน ตั้งแต่การอธิบายลักษณะพื้นฐานของข้อมูลไปจนถึงการทดสอบความสัมพันธ์เชิงเหตุและผล อันนำไปสู่ข้อสรุปเชิงประจักษ์ที่สอดคล้องกับวัตถุประสงค์และสมมติฐานของการวิจัยระดับปริญญาโทอย่างเป็นระบบ และมีความน่าเชื่อถือทางวิชาการ

บทที่ 4

ผลการวิจัย

การวิจัยเรื่อง แนวทางพัฒนาการออกแบบเทคโนโลยีความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล เพื่อสอดคล้องกับมาตรฐาน HAIT Plus และ ISO 27001 โดยผู้วิจัยได้เก็บรวบรวมข้อมูลจากกลุ่มตัวอย่างที่เป็นบุคลากรที่เกี่ยวข้องในโรงพยาบาลธรรมศาสตร์เฉลิมพระเกียรติ จำนวน 250 คน และนำข้อมูลมาประมวลผลวิเคราะห์ด้วยโปรแกรมสำเร็จรูปทางสถิติ โดยมีการนำเสนอผลการวิเคราะห์ข้อมูลตามลำดับ ดังนี้

- 4.1 ผลการวิเคราะห์ข้อมูลทั่วไป
- 4.2 ผลการวิเคราะห์ตัวแปรแต่ละด้าน
- 4.3 การวิเคราะห์องค์ประกอบเชิงสำรวจ
- 4.4 การประเมินโมเดลโครงสร้างและการทดสอบสมมติฐาน

4.1 ผลการวิเคราะห์ข้อมูลทั่วไป

ในการวิเคราะห์ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ผู้วิจัยได้นำเสนอข้อมูลลักษณะทางประชากรศาสตร์ของกลุ่มตัวอย่าง ได้แก่ เพศ อายุ ระดับการศึกษา ฝาย และประสบการณ์การทำงาน โดยใช้สถิติเชิงพรรณนาในการวิเคราะห์ ได้แก่ การแจกแจงความถี่ (Frequency) และค่าร้อยละ (Percentage) นอกจากนี้ ผู้วิจัยได้จัดกลุ่มองค์กรตามลักษณะอุตสาหกรรมหลัก โดยรวมประเภทที่มีจำนวนผู้ตอบน้อยเข้ากลุ่ม Other Technology-related เพื่อความเหมาะสมในการนำเสนอข้อมูล ดังแสดงในตารางที่ 4-1

ตารางที่ 4-1 จำนวนและร้อยละของข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

ข้อมูลทั่วไป	จำนวน (คน)	ร้อยละ (%)
เพศ (Gender)		
ชาย	90	36.00
หญิง	133	53.20
ไม่ระบุ / ทางเลือกอื่น	27	10.80
รวม	250	100.00

ตารางที่ 4-1 (ต่อ)

ข้อมูลทั่วไป	จำนวน (คน)	ร้อยละ (%)
อายุ (Age)		
18 - 30 ปี	45	18.00
31 - 40 ปี	105	42.00
41 - 50 ปี	62	24.80
51 - 60 ปี	37	14.80
60 - 70 ปี	1	0.40
มากกว่า 70 ปี	0	0.00
รวม	250	100.00
ระดับการศึกษา (Education)		
ปริญญาเอก	6	2.40
ปริญญาโท	72	28.80
ปริญญาตรี	157	62.80
มัธยมศึกษาตอนปลาย/อนุปริญญา	13	5.20
มัธยมศึกษาตอนต้น	2	0.80
ต่ำกว่ามัธยมศึกษา	0	0.00
รวม	250	100.00
สังกัดฝ่าย		
ฝ่ายบริหาร	27	10.80
ฝ่ายการแพทย์/ห้องปฏิบัติการ	54	21.60
ฝ่ายการพยาบาล	74	29.60
ฝ่ายเทคโนโลยีสารสนเทศ	34	13.60
ฝ่ายการเงิน/ธุรการ	2	0.80
ฝ่ายเภสัชกรรม	19	7.60
ฝ่ายคุณภาพ	20	8.00
รวม	250	100.00
ประสบการณ์ทำงาน/ความรู้ด้านความมั่นคง ปลอดภัยทางไซเบอร์		
1-3 ปี	88	35.20
4-6 ปี	96	38.40
7 ปีขึ้นไป	42	16.80
ไม่มีประสบการณ์	24	9.60
รวม	250	100.00

จากตาราง 4-1 จากการศึกษากลุ่มตัวอย่างทั้งหมด 250 คน พบว่า กลุ่มตัวอย่างส่วนใหญ่เป็นเพศหญิงจำนวน 133 คน คิดเป็นร้อยละ 53.20 เพศชายจำนวน 90 คน คิดเป็นร้อยละ 36.00 และไม่ระบุเพศ จำนวน 27 คน คิดเป็นร้อยละ 10.80%

ช่วงอายุของกลุ่มตัวอย่างส่วนใหญ่จะอยู่ช่วงอายุ 31-40 ปี คิดเป็นร้อยละ 42.00 รองลงมาเป็นช่วงอายุ 41-50 ปี คิดเป็นร้อยละ อันดับที่สามเป็นช่วงอายุ 18-30 ปี คิดเป็นร้อยละ 18.00 อันดับที่เป็นช่วงอายุ 51-60 ปี คิดเป็นร้อยละ 14.8 และอันดับห้าเป็นช่วงอายุ 60-70 ปี คิดเป็นร้อยละ 0.40 และช่วงอายุมากกว่า 70 ปี จะไม่มีผู้ตอบแบบสอบถาม

ระดับการศึกษาของผู้ตอบแบบสอบถามโดยส่วนมากจะอยู่ในระดับปริญญาตรี จำนวน 157 คน คิดเป็นร้อยละ 62.80 อันดับที่สองระดับปริญญาโท จำนวน 72 คน คิดเป็นร้อยละ 28.80 อันดับที่สามารถระดับมัธยมศึกษาตอนปลาย/อนุปริญญา จำนวน 13 คน คิดเป็นร้อยละ 5.20 อันดับที่สามารถระดับการศึกษาปริญญาเอก จำนวน 6 คน คิดเป็นร้อยละ 2.40 และระดับมัธยมศึกษาตอนต้น จำนวน 2 คน คิดเป็นร้อยละ 0.80

สังกัดฝ่ายของผู้ตอบแบบสอบถามอันดับแรกสังกัดฝ่ายฝ่ายการพยาบาล จำนวน 74 คน คิดเป็นร้อยละ 29.60 อันดับสองสังกัดฝ่ายการแพทย์/ห้องปฏิบัติการ จำนวน 54 คน คิดเป็นร้อยละ 21.60 อันดับสามสังกัดฝ่ายเทคโนโลยีสารสนเทศ จำนวน 34 คน คิดเป็นร้อยละ 13.60 อันดับสี่สังกัดฝ่ายบริหาร จำนวน 27 คน คิดเป็นร้อยละ 10.80 อันดับห้ามีสองสังกัดฝ่ายได้แก่ ฝ่ายคุณภาพและฝ่ายอื่น จำนวน 20 คน คิดเป็นร้อยละ 8.00 และอันดับหกสังกัดฝ่ายเภสัชกรรม จำนวน 19 คน คิดเป็นร้อยละ 7.60 และอันดับสุดท้ายสังกัดฝ่ายการเงิน/ธุรการ จำนวน 2 คน คิดเป็นร้อยละ 0.80

ประสบการณ์ทำงาน/ความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของผู้ตอบแบบสอบถาม อันดับหนึ่งประสบการณ์ทำงาน/ความรู้ 4-6 ปี จำนวน 96 คน คิดเป็นร้อยละ 38.40 อันดับสอง 1-3 ปี จำนวน 88 คน คิดเป็นร้อยละ 35.20 อันดับสาม 7 ปีขึ้นไป จำนวน 42 คน คิดเป็นร้อยละ 16.80 และไม่มีประสบการณ์จำนวน 24 คน คิดเป็นร้อยละ 9.60 เป็นลำดับสุดท้าย

4.2 ผลการวิเคราะห์ตัวแปรแต่ละด้าน

ผู้วิจัยได้ทำการวิเคราะห์ระดับความคิดเห็นของกลุ่มตัวอย่างที่มีต่อปัจจัยตามกรอบแนวคิดการวิจัย โดยใช้สถิติเชิงพรรณนา ได้แก่ ค่าเฉลี่ย (Mean) ใช้ในการแสดงระดับความคิดเห็นโดยรวมของกลุ่มตัวอย่างต่อแต่ละปัจจัย ขณะที่ส่วนเบี่ยงเบนมาตรฐาน (S.D.) ใช้เพื่อแสดงระดับความแปรปรวนของความคิดเห็น หากค่าส่วนเบี่ยงเบนมาตรฐาน (S.D.) มีค่าน้อย แสดงว่าผู้ตอบมีความคิดเห็นไปในทิศทางเดียวกันค่อนข้างมาก แต่หากค่าส่วนเบี่ยงเบนมาตรฐาน (S.D.) มีค่าสูง แสดงว่าความคิดเห็นมีความแตกต่างกันมากขึ้น

ผลการวิเคราะห์รายละเอียดของแต่ละตัวแปร แสดงดังตารางที่ 4-2 ถึงตารางที่ 4-10 ซึ่งนำเสนอค่าเฉลี่ย ระดับความคิดเห็น และส่วนเบี่ยงเบนมาตรฐานของแต่ละปัจจัยตามลำดับ

4.2.1 ปัจจัยด้านความพร้อมความมั่นคงเทคโนโลยีสารสนเทศ (IT Security Readiness)

ปัจจัยด้านความพร้อมความมั่นคงเทคโนโลยีสารสนเทศ (IT Security Readiness) เป็นตัวแปรสำคัญที่สะท้อนศักยภาพเชิงโครงสร้างขององค์กรในการรองรับการดำเนินงานตามมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ โดยครอบคลุมทั้งมิติด้านนโยบาย โครงสร้างพื้นฐาน และทรัพยากร

สนับสนุน ผู้วิจัยได้ทำการวิเคราะห์ข้อมูลโดยใช้ค่าเฉลี่ย (Mean) และส่วนเบี่ยงเบนมาตรฐาน (S.D.) เพื่ออธิบายระดับความคิดเห็นของกลุ่มตัวอย่างต่อปัจจัยดังกล่าว โดยผลการวิเคราะห์แสดงรายละเอียดดังตารางที่ 4-2

ตารางที่ 4-2 ค่าเฉลี่ยและค่าส่วนเบี่ยงเบนมาตรฐานปัจจัยด้านความพร้อมความมั่นคงเทคโนโลยีสารสนเทศ

ข้อคำถาม	ค่าเฉลี่ย	S.D.	ระดับความคิดเห็น
นโยบายและระเบียบปฏิบัติ	3.94	0.72	สูง
โครงสร้างพื้นฐานเทคโนโลยี	3.88	0.76	สูง
ทรัพยากรและการสนับสนุน	3.72	0.81	สูง
รวม	3.85	0.69	สูง

จากตารางที่ 4-2 พบว่า ปัจจัยด้านความพร้อมความมั่นคงเทคโนโลยีสารสนเทศโดยรวมอยู่ในระดับ “สูง” คือ ค่าเฉลี่ย คือ 3.85 และส่วนเบี่ยงเบนมาตรฐาน คือ 0.69 สะท้อนให้เห็นว่าองค์กรมีความพร้อมเชิงโครงสร้างและเชิงนโยบายในการรองรับมาตรฐานความมั่นคงปลอดภัยในระดับที่ดี โดยเฉพาะด้านนโยบายและระเบียบปฏิบัติ ซึ่งมีค่าเฉลี่ยสูงสุด คือ 3.94 แสดงถึงความชัดเจนของแนวทางการกำกับดูแลด้านความมั่นคงปลอดภัย

อย่างไรก็ตาม ด้านทรัพยากรและการสนับสนุน มีค่าเฉลี่ยต่ำกว่าด้านอื่น ค่าเฉลี่ย คือ 3.72 และมีค่าส่วนเบี่ยงเบนมาตรฐาน คือ 0.81 สะท้อนให้เห็นถึงความแตกต่างของความคิดเห็นในประเด็นดังกล่าว ซึ่งอาจบ่งชี้ถึงข้อจำกัดด้านงบประมาณ บุคลากร หรือการสนับสนุนเชิงปฏิบัติการในบางหน่วยงาน ทั้งนี้ ประเด็นดังกล่าวควรได้รับการพิจารณาเชิงนโยบายเพื่อเสริมสร้างความพร้อมอย่างสมดุลและยั่งยืนในระยะยาว

4.2.2 ปัจจัยด้านบุคลากร (Human Factors)

ปัจจัยด้านบุคลากร (Human Factors) เป็นตัวแปรที่สะท้อนบทบาทของมนุษย์ในฐานะกลไกสำคัญของระบบความมั่นคงปลอดภัยทางไซเบอร์ เนื่องจากบุคลากรถือเป็นทั้ง “ด่านป้องกันแรก” และในบางกรณีอาจเป็น “จุดอ่อนสำคัญ” ขององค์กร หากขาดความรู้ ความตระหนัก หรือทักษะที่เหมาะสม ผู้วิจัยได้ทำการวิเคราะห์ข้อมูลโดยใช้ค่าเฉลี่ย (Mean) และส่วนเบี่ยงเบนมาตรฐาน (S.D.) เพื่ออธิบายระดับความคิดเห็นของกลุ่มตัวอย่างต่อปัจจัยดังกล่าว โดยผลการวิเคราะห์แสดงรายละเอียดดังตารางที่ 4-3

ตารางที่ 4-3 ค่าเฉลี่ยและค่าส่วนเบี่ยงเบนมาตรฐานปัจจัยด้านบุคลากร

ข้อคำถาม	ค่าเฉลี่ย	S.D.	ระดับความคิดเห็น
สมรรถนะและความรู้	3.67	0.83	สูง
ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์	4.12	0.64	สูง
รวมเฉลี่ย	3.90	0.68	สูง

จากตารางที่ 4-3 พบว่า ปัจจัยด้านบุคลากรโดยรวมอยู่ในระดับ “สูง” คือ ค่าเฉลี่ย คือ 3.90 และส่วนเบี่ยงเบนมาตรฐาน คือ 0.68 สะท้อนให้เห็นว่ากลุ่มตัวอย่างมีความคิดเห็นเชิงบวกต่อศักยภาพด้านทรัพยากรมนุษย์ขององค์กรในการรองรับมาตรการความมั่นคงปลอดภัยทางไซเบอร์

เมื่อพิจารณารายด้าน พบว่า “ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์” มีค่าเฉลี่ยสูงที่สุด คือ 4.12 และส่วนเบี่ยงเบนมาตรฐาน คือ 0.64 ซึ่งมีค่า S.D. ค่อนข้างต่ำ (0.64) แสดงให้เห็นว่าบุคลากรส่วนใหญ่มีความเข้าใจต่อความเสี่ยงและภัยคุกคามทางไซเบอร์ในระดับดีมาก และมีความคิดเห็นไปในทิศทางเดียวกันอย่างชัดเจน

อย่างไรก็ตาม ด้าน “สมรรถนะและความรู้” มีค่าเฉลี่ยต่ำกว่าองค์ประกอบอื่น (3.67) และมีค่า S.D. ค่อนข้างสูง (0.83) สะท้อนถึงความแตกต่างของระดับความรู้และทักษะเฉพาะทางในกลุ่มตัวอย่าง ซึ่งอาจเกิดจากความหลากหลายของสายงาน ประสบการณ์ หรือโอกาสในการเข้ารับการอบรมด้านความมั่นคงปลอดภัยไซเบอร์ ดังนั้น องค์กรควรพิจารณากำหนดแนวทางการพัฒนาศักยภาพบุคลากรอย่างเป็นระบบ เพื่อยกระดับความรู้เชิงลึกและลดความเหลื่อมล้ำด้านทักษะในระยะยาว

4.2.3 ปัจจัยด้านการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Perception Level)

ปัจจัยด้านการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Perception Level) เป็นตัวแปรที่สะท้อนระดับความเข้าใจ ความตระหนัก และการรับรู้ของบุคลากรต่อกรอบมาตรฐานที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในบริบทของโรงพยาบาล ซึ่งถือเป็นองค์ประกอบสำคัญในการขับเคลื่อนการปฏิบัติให้เป็นไปตามข้อกำหนดอย่างมีประสิทธิภาพ ผู้วิจัยได้ทำการวิเคราะห์ข้อมูลโดยใช้ค่าเฉลี่ย (Mean) และค่าส่วนเบี่ยงเบนมาตรฐาน (S.D.) เพื่ออธิบายระดับความคิดเห็นของกลุ่มตัวอย่างต่อปัจจัยดังกล่าว โดยผลการวิเคราะห์แสดงรายละเอียดดังตารางที่ 4-4

ตารางที่ 4-4 ค่าเฉลี่ยและค่าส่วนเบี่ยงเบนมาตรฐานปัจจัยด้านการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์

ข้อคำถาม	ค่าเฉลี่ย	S.D.	ระดับความคิดเห็น
การรับรู้มาตรฐาน HAIT Plus	3.95	0.70	สูง
การรับรู้มาตรฐาน ISO/IEC 27001	3.89	0.75	สูง
รวมเฉลี่ย	3.92	0.68	สูง

จากตารางที่ 4-4 พบว่า โดยภาพรวมกลุ่มตัวอย่างมีระดับการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์อยู่ในระดับ “สูง” ค่าเฉลี่ย คือ 3.92 และส่วนเบี่ยงเบนมาตรฐาน คือ 0.68 สะท้อนถึงความตระหนักและความเข้าใจต่อกรอบมาตรฐานที่เกี่ยวข้องในระดับที่น่าพอใจ

เมื่อพิจารณารายประเด็น พบว่า การรับรู้มาตรฐาน HAIT Plus มีค่าเฉลี่ยสูงกว่าคือ 3.95 เมื่อเทียบกับมาตรฐาน ISO/IEC 27001 ซึ่งมีค่าเฉลี่ย 3.89 แม้ทั้งสองมาตรฐานจะอยู่ในระดับ “สูง” เช่นเดียวกัน ทั้งนี้อาจสะท้อนถึงบริบทขององค์กรด้านสาธารณสุขที่มีความคุ้นเคยและมีการสื่อสารเกี่ยวกับมาตรฐาน HAIT Plus มากกว่า เนื่องจากเป็นมาตรฐานที่พัฒนาขึ้นเพื่อรองรับระบบสารสนเทศในสถานพยาบาลโดยเฉพาะ

ในขณะเดียวกัน ค่าส่วนเบี่ยงเบนมาตรฐาน ของการรับรู้ ISO/IEC 27001 ที่สูงกว่าเล็กน้อย คือ 0.75 อาจสะท้อนถึงความแตกต่างของระดับความเข้าใจในมาตรฐานสากลดังกล่าว ซึ่งมีรายละเอียดเชิงเทคนิคและข้อกำหนดเชิงระบบที่ซับซ้อนกว่า ดังนั้น องค์กรอาจพิจารณาส่งเสริม การให้ความรู้และสร้างความเข้าใจเชิงลึกเกี่ยวกับมาตรฐานสากลควบคู่กับมาตรฐานเฉพาะทางด้าน สาธารณสุข เพื่อยกระดับความพร้อมของบุคลากรในภาพรวมอย่างยั่งยืน

4.2.4 ปัจจัยด้านความพร้อมในการบริหารจัดการตามมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Implementation Readiness)

ปัจจัยด้านความพร้อมในการบริหารจัดการตามมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Implementation Readiness) เป็นตัวแปรที่สะท้อนศักยภาพขององค์กรในการแปลง “การรับรู้เชิงนโยบาย” ไปสู่ “การปฏิบัติเชิงระบบ” อย่างเป็นรูปธรรม ครอบคลุมทั้งความสามารถในการประยุกต์ใช้มาตรฐาน กระบวนการสนับสนุนภายในองค์กร และระดับความมั่นใจของบุคลากรในการดำเนินงานตามข้อกำหนด ผู้วิจัยได้ทำการวิเคราะห์ข้อมูลโดยใช้ค่าเฉลี่ย (Mean) และค่าส่วนเบี่ยงเบนมาตรฐาน (S.D.) เพื่ออธิบายระดับความคิดเห็นของกลุ่มตัวอย่างต่อปัจจัยดังกล่าว โดยผลการวิเคราะห์แสดงรายละเอียดดังตารางที่ 4-5

ตารางที่ 4-5 ค่าเฉลี่ยและค่าส่วนเบี่ยงเบนมาตรฐานปัจจัยด้านความพร้อมในการบริหารจัดการตามมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์

ข้อคำถาม	ค่าเฉลี่ย	S.D.	ระดับความคิดเห็น
ความสามารถในการนำมาตรฐานไปปฏิบัติ	3.79	0.77	สูง
ความพร้อมด้านระบบและกระบวนการ	3.82	0.74	สูง
ความมั่นใจในการดำเนินงานตามมาตรฐาน	3.69	0.81	สูง
รวมเฉลี่ย	3.77	0.77	สูง

จากตารางที่ 4-5 พบว่า ปัจจัยด้านความพร้อมในการบริหารจัดการตามมาตรฐานโดยรวมอยู่ในระดับ “สูง” ค่าเฉลี่ย คือ 3.77 และส่วนเบี่ยงเบนมาตรฐาน คือ 0.77 อย่างไรก็ตาม เมื่อเปรียบเทียบกับปัจจัยด้านการรับรู้มาตรฐานในหัวข้อก่อนหน้านี้ จะเห็นได้ว่าค่าเฉลี่ยมีระดับต่ำกว่าเล็กน้อย

ผลดังกล่าวสะท้อนให้เห็นถึง “ช่องว่างระหว่างการเรียนรู้และการปฏิบัติ” (Perception-Practice Gap) กล่าวคือ แม้บุคลากรจะมีความเข้าใจและตระหนักถึงความสำคัญของมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ในระดับสูง แต่ความพร้อมเชิงระบบและความมั่นใจในการนำไปประยุกต์ใช้จริงยังอยู่ในระดับที่ต้องการการเสริมสร้างเพิ่มเติม โดยเฉพาะด้านความมั่นใจในการดำเนินงานตามมาตรฐาน ซึ่งมีค่าเฉลี่ยต่ำที่สุด คือ 3.69 และมีค่าส่วนเบี่ยงเบนมาตรฐาน คือ 0.81 ซึ่งค่อนข้างสูงสะท้อนถึงความแตกต่างของประสบการณ์และความชำนาญในกลุ่มตัวอย่าง

ประเด็นดังกล่าวมีนัยสำคัญต่อการกำหนดกลยุทธ์องค์กร เนื่องจากการบรรลุผลตามมาตรฐานความมั่นคงปลอดภัยมิได้ขึ้นอยู่กับระดับการรับรู้เพียงอย่างเดียว หากแต่ต้องอาศัยความพร้อมเชิงโครงสร้าง กระบวนการสนับสนุนที่ชัดเจน และการพัฒนาศักยภาพบุคลากรอย่างต่อเนื่อง เพื่อให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพและยั่งยืนในระยะยาว

4.3 การวิเคราะห์องค์ประกอบเชิงสำรวจ

ผู้วิจัยได้ดำเนินการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ซึ่งเป็นขั้นตอนการยืนยันเครื่องมือวัดมีความสอดคล้องกับโครงสร้างทฤษฎีและสามารถนำไปใช้ทดสอบสมมติฐานได้อย่างเหมาะสม

4.3.1 ผลการตรวจสอบความเหมาะสมของข้อมูล

ผลการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) เพื่อสำรวจโครงสร้างของตัวแปรแฝงและตรวจสอบความสามารถของข้อคำถามในการรวมกลุ่มเป็นปัจจัยตามกรอบแนวคิดที่กำหนดหรือไม่ งานวิจัยนี้ ดำเนินการสกัดองค์ประกอบด้วยวิธี Maximum Likelihood และหมุน แกนแบบ Oblimin ซึ่งอนุญาตให้ปัจจัยมีความสัมพันธ์กันได้ ซึ่งเหมาะสมกับตัวแปรด้านการรับรู้ พฤติกรรมที่มีความสัมพันธ์กัน ผู้วิจัยได้ดำเนินการตรวจสอบสมมติฐานพื้นฐานของ EFA ได้แก่ การทดสอบความเพียงพอของขนาดตัวอย่างและความเหมาะสมของเมทริกซ์สหสัมพันธ์ผ่านสถิติ Ksiser-Meyer-Olkin (KMO) และ การวิเคราะห์ค่า Measure of Sampling Adequacy: MSA

4.3.1.1 การทดสอบความเพียงพอของขนาดตัวอย่างและความเหมาะสมของเมทริกซ์สหสัมพันธ์ผ่านสถิติ Ksiser-Meyer-Olkin (KMO) ก่อนดำเนินการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ผู้วิจัยได้ตรวจสอบความเพียงพอของขนาดตัวอย่างและความเหมาะสมของข้อมูลสำหรับการวิเคราะห์องค์ประกอบ โดยใช้สถิติ Kaiser-Meyer-Olkin (KMO) และการทดสอบ Bartlett's Test of Sphericity เพื่อประเมินว่าข้อมูลมีความสัมพันธ์กันในระดับที่เหมาะสมและสามารถสกัดองค์ประกอบรวมได้อย่างมีนัยสำคัญทางสถิติ แสดงดังตารางที่ 4-6

ตารางที่ 4-6 สรุปผล KMO และ Bartlett's Test of Sphericity ตามรอบการวิเคราะห์

รอบการวิเคราะห์	จำนวนตัวแปร	KMO (Overall)	Bartlett's χ^2	df	p-value
ครั้งที่ 1	17	0.845	1723	136	< .001
ครั้งที่ 2	16	0.841	1612	120	< .001
ครั้งที่ 3	15	0.827	1438	105	< .001
ครั้งที่ 4	14	0.827	1359	91	< .001

จากตารางที่ 4-6 พบว่า ค่า KMO ในทุกรอบการวิเคราะห์มีค่าอยู่ระหว่าง 0.827–0.845 ซึ่งอยู่ในระดับ “ดีมาก” ถึง “ยอดเยี่ยม” ตามเกณฑ์การแปลผลของ Kaiser สะท้อนให้เห็นว่าข้อมูลมีความเพียงพอและเหมาะสมต่อการวิเคราะห์องค์ประกอบเชิงสำรวจ

นอกจากนี้ ผลการทดสอบ Bartlett's Test of Sphericity พบว่ามีนัยสำคัญทางสถิติในทุกรอบการวิเคราะห์ ($p < .001$) แสดงให้เห็นว่าเมทริกซ์สหสัมพันธ์แตกต่างจากเมทริกซ์เอกลักษณ์ (Identity Matrix) อย่างมีนัยสำคัญ กล่าวคือ ตัวแปรมีความสัมพันธ์กันในระดับที่เพียงพอสำหรับการสกัดองค์ประกอบรวม

การดำเนินการวิเคราะห์จำนวน 4 รอบ มีวัตถุประสงค์เพื่อปรับปรุงคุณภาพของเครื่องมือวัดโดยการคัดเลือกข้อคำถามที่มีค่าน้ำหนักองค์ประกอบ (Factor Loading) ชัดเจน สอดคล้องกับกรอบ

แนวคิดเชิงทฤษฎี และลดปัญหา Cross-loading ตลอดจนตัดข้อคำถามที่มีค่าเอกลักษณ์ (Uniqueness) สูงเกินเกณฑ์ที่กำหนด กระบวนการดังกล่าวช่วยให้โครงสร้างองค์ประกอบที่ได้มีความกระชับ ชัดเจน และมีความเที่ยงตรงเชิงโครงสร้าง (Construct Validity) สูงขึ้น อันเป็นพื้นฐานสำคัญสำหรับการวิเคราะห์เชิงสาเหตุในขั้นตอนถัดไป

4.3.1.2 การวิเคราะห์ค่า Measure of Sampling Adequacy (MSA) รายตัวแปร
 ภายหลังจากการประเมินความเหมาะสมของข้อมูลในระดับภาพรวมด้วยค่า KMO ผู้วิจัยได้ดำเนินการวิเคราะห์ค่า Measure of Sampling Adequacy (MSA) รายตัวแปร เพื่อพิจารณาความเหมาะสมของข้อคำถามแต่ละข้อในการเข้าร่วมการวิเคราะห์องค์ประกอบเชิงสำรวจ (EFA) โดยค่า MSA เป็นดัชนีที่สะท้อนระดับความสัมพันธ์ร่วมระหว่างตัวแปรหนึ่งกับตัวแปรอื่น ๆ ในเมทริกซ์สหสัมพันธ์ หากค่ามีระดับสูง แสดงว่าตัวแปรดังกล่าวมีความเชื่อมโยงกับโครงสร้างปัจจัยร่วมอย่างเพียงพอ และมีแนวโน้มที่จะเป็นส่วนหนึ่งขององค์ประกอบแฝงเดียวกัน โดยทั่วไป ค่า MSA มากกว่า 0.50 ถือว่าอยู่ในเกณฑ์ยอมรับได้ มากกว่า 0.70 อยู่ในระดับดี และหากมีค่าเข้าใกล้ 1.00 ยิ่งสะท้อนถึงความเหมาะสมในระดับสูง แสดงดังตารางที่ 4-7

ตารางที่ 4-7 สรุปช่วงค่า MSA รายตัวแปรและข้อสังเกตจำแนกตามรอบการวิเคราะห์

รอบการวิเคราะห์	ช่วงค่า MSA รายตัวแปร (ต่ำสุด-สูงสุด)	ข้อที่มี MSA ต่ำสุด	ข้อที่มี MSA สูงสุด
ครั้งที่ 1	0.755-0.919	SP(13)	Dev(18)
ครั้งที่ 2	0.761-0.916	Dev(16)	Dev(18)
ครั้งที่ 3	0.759-0.892	Dev(16)	Dev(18)
ครั้งที่ 4	0.748-0.894	Dev(16)	Dev(18)

จากตารางที่ 4-7 พบว่า ค่า MSA รายตัวแปรของทุกข้อมีค่ามากกว่า 0.70 ในภาพรวมตลอดทุกรอบการวิเคราะห์ โดยมีช่วงค่าระหว่าง 0.748–0.919 ซึ่งอยู่ในระดับ “ดี” ถึง “ดีมาก” สะท้อนถึงความเหมาะสมของข้อคำถามทั้งหมดต่อการวิเคราะห์องค์ประกอบ

ข้อ Dev(18) มีค่า MSA สูงที่สุดอย่างต่อเนื่องในทุกรอบการวิเคราะห์ แสดงให้เห็นว่าข้อคำถามดังกล่าวมีความสัมพันธ์ร่วมกับตัวแปรอื่นในชุดเดียวกันอย่างเด่นชัด และมีศักยภาพสูงในการเป็นตัวแทนของโครงสร้างองค์ประกอบแฝง ขณะที่ข้อที่มีค่า MSA ต่ำสุดในแต่ละรอบยังคงมีค่ามากกว่า 0.74 ซึ่งจัดอยู่ในเกณฑ์ดี ไม่ปรากฏข้อคำถามใดที่มีค่า MSA ต่ำกว่าเกณฑ์มาตรฐานที่ควรพิจารณาตัดออก

ดังนั้น จึงสรุปได้ว่า ไม่มีข้อคำถามใดที่จำเป็นต้องตัดออกด้วยเหตุผลด้านค่า MSA เพียงอย่างเดียว อย่างไรก็ตาม การคัดเลือกข้อคำถามเข้าสู่โมเดลองค์ประกอบขั้นสุดท้ายยังต้องพิจารณาร่วมกับค่าน้ำหนักองค์ประกอบ (Factor Loading) ความชัดเจนของการจัดกลุ่ม (Factor Structure) ปัญหา Cross-loading และความสอดคล้องเชิงทฤษฎี เพื่อให้โครงสร้างเครื่องมือวัดมีความเที่ยงตรงเชิงโครงสร้างและมีความแข็งแกร่งทางวิชาการในขั้นตอนการวิเคราะห์ต่อไป

4.3.2 ผลการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) และการปรับแบบจำลองรายรอบ

ผู้วิจัยได้ดำเนินการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) เพื่อศึกษารูปแบบโครงสร้างองค์ประกอบแฝงของตัวแปร และตรวจสอบความสอดคล้องของข้อคำถามกับกรอบแนวคิดเชิงทฤษฎี โดยทำการสกัดองค์ประกอบ (Factor Extraction) และพิจารณาค่าน้ำหนักองค์ประกอบ (Factor Loadings) ในแต่ละรอบการวิเคราะห์รวมทั้งสิ้น 4 ครั้ง เกณฑ์ที่ใช้ในการพิจารณาความเหมาะสมของข้อคำถามในเชิงปฏิบัติ ประกอบด้วย

1. ค่าน้ำหนักองค์ประกอบควรมีขนาดเพียงพอและชัดเจนกับปัจจัยใดปัจจัยหนึ่ง
2. หลีกเลี่ยงการเกิด Cross-loading กล่าวคือ ข้อคำถามไม่ควรมีค่าน้ำหนักใกล้เคียงกันในหลายปัจจัย
3. พิจารณาค่า Uniqueness ซึ่งสะท้อนสัดส่วนความแปรปรวนของข้อคำถามที่ไม่สามารถอธิบายได้ด้วยปัจจัยร่วม หากมีค่าสูงมาก แสดงว่าข้อคำถามอาจไม่สอดคล้องกับโครงสร้างองค์ประกอบโดยรวม

ในการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ใช้ตัวแปรรวมทั้งสิ้น 17 ข้อ ครอบคลุม 5 มิติ ได้แก่

1. ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA)
2. การสนับสนุนจากองค์กร (Support from Organization: SP)
3. การรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (Perceived Usefulness: PU)
4. ความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats (CT)
5. ความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev)

4.3.2.1 ผลการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ครั้งที่ 1 ผลการวิเคราะห์รอบที่ 1 แสดงให้เห็นว่าข้อคำถามส่วนใหญ่มีค่าน้ำหนักองค์ประกอบอยู่ในระดับค่อนข้างสูงในปัจจัยที่เกี่ยวข้อง สะท้อนถึงความสอดคล้องเบื้องต้นกับโครงสร้างเชิงทฤษฎี อย่างไรก็ตาม มีบางข้อปรากฏลักษณะ Cross-loading ซึ่งบ่งชี้ถึงความไม่ชัดเจนของมิติที่ต้องการวัด แสดงดังตารางที่ 4-8

ตารางที่ 4-8 สรุปน้ำหนักองค์ประกอบและค่า Uniqueness จากการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ครั้งที่ 1

ตัวแปร	ปัจจัยเด่น (Loading)	Uniqueness
SA(6)	0.750	0.363
SA(8)	0.654	0.475
SP(10)	0.851	0.273
SP(11)	0.530	0.660
SP(12)	0.414	0.680
SP(13)	0.436 (มี Cross-loading)	0.525
PU(7)	0.780	0.396
PU(9)	0.373 และ -0.444	0.466

ตารางที่ 4-8 (ต่อ)

ตัวแปร	ปัจจัยเด่น (Loading)	Uniqueness
Ct(14)	0.670	0.333
Ct(15)	0.613	0.531
Dev(16)	0.753	0.348
Dev(17)	0.848	0.325
Dev(18)	0.730	0.512
Dev(19)	0.858	0.236
Dev(20)	0.766	0.273
Dev(21)	0.685	0.496
Dev(22)	0.684	0.556

จากตารางที่ 4-8 เมื่อพิจารณาในเชิงเทคนิค พบว่าข้อที่ควรให้ความสำคัญเป็นพิเศษ ได้แก่ PU(9) ซึ่งมีการโหลดในหลายปัจจัยและมีทิศทางของค่าน้ำหนักทั้งเชิงบวกและเชิงลบ คือ 0.373 และ -0.444 สะท้อนถึงความกำกวมเชิงเนื้อหา หรืออาจวัดมิติที่ทับซ้อนกับปัจจัยอื่น นอกจากนี้ SP(13) ยังปรากฏลักษณะ Cross-loading เช่นเดียวกัน แม้จะมีค่าน้ำหนักไม่สูงมาก

ในขณะเดียวกันมิติความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) ส่วนใหญ่มีค่าน้ำหนักองค์ประกอบสูงและค่า Uniqueness ต่ำกว่า 0.50 หลายข้อ (เช่น Dev(19), Dev(20)) แสดงถึงความสามารถในการอธิบายด้วยปัจจัยร่วมได้ดี และมีเสถียรภาพเชิงโครงสร้างในระดับที่น่าพอใจ

อย่างไรก็ตาม การตัดสินใจคัดออกข้อคำถามใดมิได้พิจารณาเฉพาะเกณฑ์ทางสถิติเท่านั้น แต่ต้องพิจารณาร่วมกับความสอดคล้องเชิงทฤษฎี ความครบถ้วนของมิติ และผลกระทบต่อโครงสร้างองค์ประกอบโดยรวม เพื่อให้ได้แบบจำลองที่มีทั้งความเหมาะสมเชิงสถิติและความแข็งแรงเชิงแนวคิดในรอบการวิเคราะห์ถัดไป

4.3.2.2 ผลการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ครั้งที่ 2 ในการวิเคราะห์องค์ประกอบเชิงสำรวจครั้งที่ 2 ผู้วิจัยได้ปรับลดจำนวนตัวแปรจาก 17 ข้อ เหลือ 16 ข้อ โดยนำข้อคำถามที่มีปัญหาเชิงโครงสร้างในรอบแรกออกจากแบบจำลอง เพื่อเพิ่มความชัดเจนของโครงสร้างองค์ประกอบและลดปัญหา Cross-loading

ผลการตรวจสอบความเหมาะสมของข้อมูลยังคงอยู่ในระดับดีมาก ($KMO = 0.841$) และ Bartlett's Test of Sphericity มีนัยสำคัญทางสถิติ ($p < .001$) แสดงว่าข้อมูลมีความเหมาะสมสำหรับการวิเคราะห์องค์ประกอบต่อไป และโครงสร้างปัจจัยมีแนวโน้มกระชับและชัดเจนมากขึ้นเมื่อเทียบกับรอบแรก แสดงดังตารางที่ 4-9

ตารางที่ 4-9 สรุปน้ำหนักองค์ประกอบและค่า Uniqueness จากการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ครั้งที่ 2

ตัวแปร	ปัจจัยเด่น (Loading)	Uniqueness
SA(6)	0.747	0.357
SA(8)	0.648	0.477
SP(10)	0.734	0.414
SP(11)	0.617	0.611
SP(12)	0.352	0.692
SP(13)	0.529	0.647
PU(7)	0.768	0.398
Ct(14)	0.390	0.736
Ct(15)	0.690	0.534
Dev(16)	0.823	0.296
Dev(17)	0.759	0.413

ตารางที่ 4-9 (ต่อ)

ตัวแปร	ปัจจัยเด่น (Loading)	Uniqueness
Dev(18)	0.624	0.525
Dev(19)	0.839	0.235
Dev(20)	0.873	0.211
Dev(21)	0.409 (มี Cross-loading)	0.477
Dev(22)	0.939	0.071

จากตารางที่ 4-9 พบว่า โครงสร้างองค์ประกอบโดยรวมมีความชัดเจนมากขึ้น โดยเฉพาะกลุ่มตัวแปรในมิติความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) ซึ่งส่วนใหญ่มีค่าน้ำหนักองค์ประกอบสูงและค่า Uniqueness ต่ำ สะท้อนถึงความสามารถของปัจจัยร่วมในการอธิบายความแปรปรวนของข้อคำถามได้ดี

อย่างไรก็ตาม ข้อ CT(14) ซึ่งสะท้อนความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ มีค่าน้ำหนักองค์ประกอบค่อนข้างต่ำ คือ 0.390 และมีค่า Uniqueness สูง คือ 0.736 แสดงว่าปัจจัยร่วมสามารถอธิบายความแปรปรวนของข้อคำถามนี้ได้จำกัด จึงเป็นข้อที่ควรพิจารณาอย่างรอบคอบในการปรับแบบจำลองรอบถัดไป เพื่อเพิ่มความชัดเจนของมิติความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT)

ในขณะเดียวกัน Dev(22) มีค่าน้ำหนักองค์ประกอบสูงมาก คือ 0.939 และมีค่า Uniqueness ต่ำมาก คือ 0.071 แสดงให้เห็นว่าเป็นตัวแทนที่แข็งแกร่งของมิติความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) และมีบทบาทสำคัญในการสะท้อนโครงสร้างองค์ประกอบของปัจจัยดังกล่าวอย่างเด่นชัด

ดังนั้น ผลการวิเคราะห์รอบที่ 2 แสดงให้เห็นถึงพัฒนาการของแบบจำลองที่มีความกระชับและมีเสถียรภาพมากขึ้น อย่างไรก็ตาม ยังมีบางข้อคำถามที่ต้องพิจารณาปรับปรุงหรือคัดออกเพิ่มเติมเพื่อให้โครงสร้างองค์ประกอบมีความชัดเจน สอดคล้องเชิงทฤษฎี และมีคุณภาพเชิงจิตพิสัยที่เหมาะสมยิ่งขึ้นในรอบการวิเคราะห์ถัดไป

4.3.2.3 ผลการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ครั้งที่ 3 ในการวิเคราะห์องค์ประกอบเชิงสำรวจครั้งที่ 3 ผู้วิจัยได้ปรับลดจำนวนตัวแปรเหลือ 15 ข้อ โดยตัดข้อคำถามที่มีปัญหาเชิงโครงสร้างออกเพิ่มเติมจากรอบก่อนหน้า เพื่อเพิ่มความกระชับและเสถียรภาพของแบบจำลอง ผลการทดสอบความเหมาะสมของข้อมูลยังคงยืนยันความเพียงพอสำหรับการวิเคราะห์องค์ประกอบ ($KMO = 0.827$) และ Bartlett's Test of Sphericity มีนัยสำคัญทางสถิติ ($p < .001$) แสดงให้เห็นว่าตัวแปรมีความสัมพันธ์ร่วมกันอย่างเหมาะสมสำหรับการสกัดองค์ประกอบผลการวิเคราะห์แสดงดังตารางที่ 4-10

ตารางที่ 4-10 สรุปน้ำหนักองค์ประกอบและค่า Uniqueness จากการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ครั้งที่ 3

ตัวแปร	ปัจจัยเด่น (Loading)	Uniqueness
SA(6)	0.772	0.355
SA(8)	0.635	0.494
SP(10)	1.002	0.005
SP(11)	0.379	0.725
SP(12)	0.405	0.685
SP(13)	0.757	0.426
PU(7)	0.778	0.396
Ct(14)	0.731	-
Ct(15)	0.418 (มีโหลดในปัจจัยอื่น)	0.553
Dev(16)	1.002	0.005
Dev(17)	0.458 (มีโหลดอื่น)	0.489
Dev(18)	0.719	0.520
Dev(19)	0.901	0.195
Dev(20)	0.763	0.269
Dev(22)	0.604	0.590

จากตารางที่ 4-10 พบว่า โครงสร้างองค์ประกอบมีความชัดเจนมากขึ้นเมื่อเทียบกับรอบก่อนหน้า โดยเฉพาะในกลุ่มตัวแปรด้านความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) และความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA)

ซึ่งมีค่าน้ำหนักองค์ประกอบในระดับสูงอย่างต่อเนื่อง

อย่างไรก็ตาม มีบางตัวแปรที่มีค่าน้ำหนักองค์ประกอบสูงมากเกินไป 1.00 ได้แก่ SP(10) และ Dev(16) ซึ่งอาจเป็นผลจากวิธีการหมุนแกน (Rotation Method) และระดับความสัมพันธ์ระหว่างตัวแปรภายในโมเดล ในเชิงเทคนิค ค่าน้ำหนักลักษณะนี้สามารถเกิดขึ้นได้ในกรณีที่การใช้การหมุนแกนแบบเอียง (Oblique Rotation) แต่ผู้วิจัยจำเป็นต้องพิจารณาความสมเหตุสมผลเชิงเนื้อหาและความสอดคล้องทางทฤษฎีประกอบการตัดสินใจ

นอกจากนี้ CT(15) และ Dev(17) ยังคงปรากฏลักษณะ Cross-loading ซึ่งสะท้อนถึงความไม่ชัดเจนของมิติที่ข้อคำถามดังกล่าวสังกัดอยู่ และอาจส่งผลกระทบต่อความบริสุทธิ์ขององค์ประกอบ (Factor Purity) ในภาพรวม ดังนั้น ข้อคำถามดังกล่าวจึงเป็นประเด็นสำคัญที่ควรพิจารณาปรับปรุงหรือคัดออกในรอบสุดท้าย เพื่อให้โครงสร้างปัจจัยมีความชัดเจน กระชับ และง่ายต่อการตีความในเชิงทฤษฎีและเชิงปฏิบัติ

โดยสรุป ผลการวิเคราะห์ครั้งที่ 3 แสดงให้เห็นถึงพัฒนาการของแบบจำลองที่มีเสถียรภาพมากขึ้น และเข้าใกล้โครงสร้างองค์ประกอบที่เหมาะสมสำหรับการสรุปผลและนำไปใช้ในขั้นตอนการวิเคราะห์ขั้นสูงต่อไป

4.3.2.4 ผลการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ครั้งที่ 4 ในการวิเคราะห์องค์ประกอบเชิงสำรวจครั้งที่ 4 ผู้วิจัยได้คัดเลือกเฉพาะข้อคำถามที่มีคุณภาพเชิงสถิติและมีความสอดคล้องเชิงทฤษฎี เหลือจำนวนทั้งสิ้น 14 ข้อ เพื่อให้ได้แบบจำลองที่มีความกระชับ ชัดเจน และตีความได้ง่ายยิ่งขึ้น ผลการทดสอบความเหมาะสมของข้อมูลพบว่าค่า KMO เท่ากับ 0.827 และ Bartlett's Test of Sphericity มีนัยสำคัญทางสถิติ ($p < .001$) ยืนยันว่าข้อมูลมีความเหมาะสมสำหรับการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ผลการวิเคราะห์แสดงดังตารางที่ 4-11

ตารางที่ 4-11 สรุปน้ำหนักองค์ประกอบและค่า Uniqueness จากการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ครั้งที่ 4

มิติ/ปัจจัย	ข้อคำถามที่คงอยู่	ช่วง Loading เด่น (โดยสรุป)
SA	SA(6), SA(8)	0.644-0.751
Sp	SP(10), SP(11), SP(12), SP(13)	0.354-0.699
PU	PU(7)	0.767
Ct	Ct(15)	0.692
Dev	Dev(16), Dev(17), Dev(18), Dev(19), Dev(20), Dev(22)	0.634-0.979

จากตารางที่ 4-11 พบว่า แบบจำลองสุดท้ายสามารถสะท้อนโครงสร้างตามกรอบแนวคิดการวิจัยได้โดยรวม โดยเฉพาะมิติ ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) การสนับสนุนจากองค์กร (Support from Organization: SP) และ ความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) ซึ่งยังคงมีจำนวนข้อ

คำถามเพียงพอและมีค่าน้ำหนักองค์ประกอบในระดับที่ชัดเจน สะท้อนถึงความแข็งแกร่งเชิงโครงสร้างขององค์ประกอบดังกล่าว

อย่างไรก็ตาม มิติการรับรู้ประโยชน์ในการนำมาตราฐานมาใช้ (Perceived Usefulness: PU) และ ความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) เหลือเพียงมิติละ 1 ข้อในแบบจำลองสุดท้าย แม้ว่าข้อคำถามดังกล่าวจะมีค่าน้ำหนักองค์ประกอบอยู่ในระดับที่เหมาะสม ($PU = 0.767$ และ $CT = 0.692$) แต่ในเชิงจิตมิติ (Psychometrics) การมีเพียงหนึ่งข้อคำถามต่อหนึ่งองค์ประกอบอาจก่อให้เกิดข้อจำกัดด้านความเที่ยง (Reliability) และความครอบคลุมของเนื้อหา (Content Coverage) เนื่องจากไม่สามารถประเมินความสอดคล้องภายใน (Internal Consistency) ของมิตินั้นได้อย่างเต็มที่

ดังนั้น แม้แบบจำลองสุดท้ายจะมีความเหมาะสมเชิงสถิติและสอดคล้องกับกรอบแนวคิดการวิจัยในภาพรวม แต่ผู้วิจัยควรอภิปรายข้อจำกัดดังกล่าวในบทที่ 5 พร้อมเสนอแนวทางพัฒนาเครื่องมือวัดในอนาคต เช่น การเพิ่มจำนวนข้อคำถามในมิติ PU และ CT เพื่อเสริมสร้างความแข็งแกร่งเชิงโครงสร้างและความน่าเชื่อถือของเครื่องมือวิจัยในระยะยาว

4.4 ผลการทดสอบสมมติฐานด้วยการวิเคราะห์การถดถอยเชิงเส้น

การทดสอบสมมติฐานในบทนี้มุ่งเน้นตรวจสอบความสัมพันธ์เชิงเหตุและผลระหว่าง ตัวแปรต้น (Independent Variables) และ ตัวแปรตาม (Dependent Variables) ที่กำหนดในกรอบแนวคิดการวิจัย โดยอาศัยวิธีการ ถดถอยเชิงเส้นพหุคูณ (Multiple Linear Regression Analysis) ซึ่งเหมาะสมกับบริบทการวิจัยที่มีตัวแปรต้นมากกว่าหนึ่งตัวแปร และต้องการอธิบายอิทธิพลเชิงเส้นต่อผลลัพธ์ที่เป็นเชิงปริมาณ ในงานวิจัยนี้ ตัวแปรต้นที่ใช้ในการวิเคราะห์ ประกอบด้วย ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) และการสนับสนุนจากองค์กร (Support from Organization: SP)

ซึ่งทั้งสองตัวแปรอยู่ภายใต้กลุ่มปัจจัยด้านบุคลากรและด้านทรัพยากรตามที่กำหนดไว้ในเอกสารตัวแปร โดยเฉพาะในส่วนของ “ปัจจัยด้านบุคลากร (Human Factors)” และ “ทรัพยากรและการสนับสนุน (Resources & Support)” ซึ่งมีบทบาทสำคัญต่อความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร ส่วนตัวแปรตาม ประกอบด้วย 3 มิติหลัก ได้แก่ การรับรู้ประโยชน์ (Perceived Usefulness: PU) ความสามารถในการควบคุม (Perceived Control: Ct) ความต้องการพัฒนาระบบ (Need for System Development: Dev)

ซึ่งสะท้อน “ระดับการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์” และ “ความพร้อมในการบริหารจัดการตามมาตรฐาน” ตามกรอบแนวคิดด้าน IT Security Readiness และ Human Factors

ดังนั้น การวิเคราะห์ถดถอยเชิงเส้นพหุคูณในบทนี้ จึงมีเป้าหมายเพื่อตรวจสอบว่าความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) และ การสนับสนุนจากองค์กร (Support from Organization: SP) สามารถอธิบายความแปรปรวนของ การรับรู้ประโยชน์ในการนำมาตราฐานมาใช้ (Perceived Usefulness: PU) ความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats (CT) และความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัย

ทางไซเบอร์ (Development Intention: Dev) ได้มาน้อยเพียงใด รวมถึงตรวจสอบว่าทิศทางของความสัมพันธ์เป็นไปตามที่กำหนดไว้ในสมมติฐานหรือไม่

4.4.1 วิธีการวิเคราะห์และการตรวจสอบสมมติฐานของโมเดลถดถอย

ก่อนดำเนินการทดสอบสมมติฐาน ผู้วิจัยได้ตรวจสอบความเหมาะสมของข้อมูลและเงื่อนไขพื้นฐานของการใช้สถิติถดถอยเชิงเส้นพหุคูณ เพื่อให้ผลการวิเคราะห์มีความน่าเชื่อถือและสามารถตีความได้อย่างถูกต้อง โดยพิจารณาสมมติฐานสำคัญของโมเดล ดังนี้

4.4.1.1 สมมติฐานเชิงเส้น (Linearity) ผู้วิจัยพิจารณาความสัมพันธ์ระหว่างตัวแปรต้น (SA, Sp) กับตัวแปรตามแต่ละตัว (PU, Ct, Dev) ว่ามีแนวโน้มเชิงเส้นหรือไม่ โดยพิจารณาจากกราฟกระจาย (Scatter Plot) และความสอดคล้องระหว่างค่าคาดการณ์ (Predicted Values) กับค่าจริง (Observed Values) ของตัวแปรตาม ผลการตรวจสอบพบว่าความสัมพันธ์โดยรวมมีลักษณะเชิงเส้นในระดับที่ยอมรับได้ จึงสามารถประมาณค่าได้ด้วยสมการถดถอยเชิงเส้น

4.4.1.3 สมมติฐานความเป็นอิสระของค่าคลาดเคลื่อน (Independence of Errors) ค่าคลาดเคลื่อน (Residuals) จากโมเดลถดถอยถูกตรวจสอบความเป็นอิสระโดยใช้สถิติ Durbin-Watson ซึ่งเป็นดัชนีชี้วัดการเกิดอัตสหสัมพันธ์ (Autocorrelation) ของค่าคลาดเคลื่อน หากค่าอยู่ใกล้ 2 แสดงถึงความเป็นอิสระในระดับที่เหมาะสม ทั้งนี้ ความเป็นอิสระของค่าคลาดเคลื่อนเป็นเงื่อนไขสำคัญที่ทำให้การประมาณค่าสัมประสิทธิ์ด้วยวิธี Ordinary Least Squares (OLS) มีความเที่ยงตรงและมีประสิทธิภาพ

4.4.1.4 สมมติฐานความแปรปรวนเท่ากัน (Homoscedasticity) ผู้วิจัยพิจารณาการกระจายของค่าคลาดเคลื่อนเทียบกับค่าคาดการณ์ หากไม่ปรากฏรูปแบบการกระจายแบบลิ้มหรือพัด (Fan Shape) และมีการกระจายอย่างสม่ำเสมอในทุกช่วงของค่าคาดการณ์ แสดงว่าความแปรปรวนของค่าคลาดเคลื่อนมีความคงที่ ซึ่งเป็นข้อกำหนดพื้นฐานของการใช้วิธี Ordinary Least Squares (OLS) ผลการตรวจสอบพบว่าไม่ปรากฏรูปแบบที่บ่งชี้ถึงปัญหา Heteroscedasticity อย่างชัดเจน

4.4.1.5 สมมติฐานการแจกแจงปกติของค่าคลาดเคลื่อน (Normality of Errors) การตรวจสอบการแจกแจงของค่าคลาดเคลื่อนดำเนินการผ่านฮิสโตแกรม (Histogram) และกราฟ Normal Probability Plot (P-P Plot) หากค่าคลาดเคลื่อนเรียงตัวใกล้เคียงเส้นทแยงมุม และรูปทรงของการแจกแจงใกล้เคียงโค้งปกติ แสดงว่าสมมติฐานการแจกแจงปกติได้รับการสนับสนุนในระดับที่ยอมรับได้ ซึ่งมีความสำคัญต่อความถูกต้องของการทดสอบนัยสำคัญทางสถิติของค่า t และค่า F

4.4.1.6 การตรวจสอบปัญหาพหุสหสัมพันธ์ (Multicollinearity) เนื่องจากโมเดลถดถอยในงานวิจัยนี้ใช้ตัวแปรต้น 2 ตัว ได้แก่ ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness : SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) ผู้วิจัยได้ตรวจสอบปัญหาความสัมพันธ์พหุสหสัมพันธ์โดยใช้ค่า Variance Inflation Factor (VIF) และค่า Tolerance หากค่า VIF ต่ำกว่าเกณฑ์วิกฤต (เช่น ไม่เกิน 5) และค่า Tolerance มีค่ามากกว่า 0.20 แสดงว่าตัวแปรต้นไม่มีความสัมพันธ์ซ้ำซ้อนในระดับที่ส่งผลกระทบต่อความน่าเชื่อถือของค่าสัมประสิทธิ์ถดถอย

จากการตรวจสอบสมมติฐานเบื้องต้นทั้งหมด พบว่าเงื่อนไขของโมเดลถดถอยเชิงเส้นพหุคูณได้รับการสนับสนุนในระดับที่เหมาะสม จึงสามารถดำเนินการวิเคราะห์และทดสอบสมมติฐานเชิงสถิติในขั้นตอนถัดไปได้อย่างมีความเชื่อมั่นในความถูกต้องของผลการประมาณค่า

4.4.2 การทดสอบสมมติฐาน

ภายหลังจากการตรวจสอบความเหมาะสมของโมเดลถดถอยและยืนยันว่าข้อมูลเป็นไปตามข้อสมมติฐานพื้นฐานของการวิเคราะห์แล้ว ขั้นตอนต่อไปคือการทดสอบสมมติฐานการวิจัยตามกรอบแนวคิดที่กำหนดไว้ โดยใช้การวิเคราะห์ถดถอยเชิงเส้นพหุคูณ (Multiple Linear Regression Analysis) เพื่อประเมินอิทธิพลของตัวแปรต้น ได้แก่ ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) ที่มีต่อตัวแปรตามแต่ละมิติ

การนำเสนอผลการทดสอบสมมติฐานในส่วนนี้จะแยกตามตัวแปรตามแต่ละตัว ได้แก่ การรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (Perceived Usefulness: PU) ความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) และความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) โดยจะรายงานทั้งความเหมาะสมของโมเดลโดยรวม (Model Fit) ค่าสัมประสิทธิ์การตัดสินใจ (R^2) และค่าสัมประสิทธิ์ถดถอยของตัวแปรอิสระแต่ละตัว พร้อมทั้งแปลความหมายเชิงสถิติและเชิงทฤษฎีอย่างเป็นระบบ

4.4.2.1 สมมติฐานที่ 1: ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลเชิงบวกต่อการรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (Perceived Usefulness: PU) ของมาตรการ/มาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ ผลการวิเคราะห์ถดถอยเชิงเส้นพหุคูณแสดงดังตารางที่ 4-12

ตารางที่ 4-12 ผลการวิเคราะห์ถดถอยพหุคูณของตัวแปร ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (SA) และการสนับสนุนจากองค์กร (SP) ที่มีต่อการรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (PU)

รายการ	ค่าประมาณ	รายละเอียด
R	0.681	ระดับความสัมพันธ์รวมระหว่าง SA, SP กับ PU
R^2	0.464	อธิบายความแปรปรวนของ PU ได้ร้อยละ 46.4
Adjusted R^2	0.460	ปรับค่าความแม่นยำตามจำนวนตัวแปร
RMSE	0.348	ค่าคลาดเคลื่อนมาตรฐานของโมเดล
F (df1 = 2, df2 = 247)	107.00	ทดสอบความเหมาะสมของโมเดลโดยรวม
Sig. (p)	< .001	โมเดลมีนัยสำคัญทางสถิติที่ระดับ .001

จากตารางที่ 4-12 พบว่า ผลการวิเคราะห์ถดถอยเชิงเส้นพหุคูณพบว่า โมเดลที่ใช้ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) เป็นตัวแปรต้นในการทำนายการรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (Perceived Usefulness: PU) มีค่า R คือ 0.681 และค่า R^2 คือ 0.464 แสดงว่าตัว

แปรอิสระทั้งสองสามารถอธิบายความแปรปรวนของการรับรู้ประโยชน์ได้ร้อยละ 46.4 ซึ่งถือว่าอยู่ในระดับปานกลางค่อนข้างสูงสำหรับการวิจัยเชิงพฤติกรรมของบุคลากรในองค์กร

ค่า F คือ 107 และมีระดับนัยสำคัญทางสถิติที่ $p < .001$ แสดงว่าโมเดลถดถอยโดยรวมมีความเหมาะสม มีความแตกต่างอย่างมีนัยสำคัญจากโมเดลที่ไม่มีตัวแปรทำนาย (Null Model) กล่าวคือ ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) เมื่อรวมกันแล้วมีศักยภาพในการทำนายการรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (Perceived Usefulness: PU) ได้อย่างมีนัยสำคัญทางสถิติ

ค่าสัมประสิทธิ์ถดถอยของตัวแปรอิสระ แสดงดังตารางที่ 4-13

ตารางที่ 4-13 ค่าสัมประสิทธิ์ถดถอยของตัวแปรอิสระ ของตัวแปรความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (SA) และการสนับสนุนจากองค์กร (SP) ที่มีต่อการรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (PU)

ตัวแปร	b (Estimate)	SE	t	p	β	ทิศทาง/นัยสำคัญ
Intercept	1.120	0.2893	3.87	<.001	-	มีนัยสำคัญ
SA	0.635	0.0496	12.81	<.001	0.630	เชิงบวก มีนัยสำคัญ
SP	0.155	0.0598	2.59	0.010	0.127	เชิงบวก มีนัยสำคัญ

จากตารางที่ 4-13 พบว่า ค่าสัมประสิทธิ์ถดถอยของตัวแปรอิสระ ของตัวแปรความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) ที่มีต่อการรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (Perceived Usefulness: PU)

ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) มีค่าสัมประสิทธิ์ไม่มาตรฐาน (b) เท่ากับ 0.635 และมีค่า β มาตรฐานเท่ากับ 0.630 โดยมีนัยสำคัญทางสถิติที่ระดับ $p < .001$ แสดงว่าเมื่อ ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) เพิ่มขึ้น 1 หน่วย ค่าเฉลี่ยของการรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (Perceived Usefulness: PU) จะเพิ่มขึ้น 0.635 หน่วย ภายใต้เงื่อนไขที่การสนับสนุนจากองค์กร (Support from Organization: SP) คงที่ และเมื่อพิจารณาค่า β พบว่าความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) เป็นตัวแปรที่มีอิทธิพลสูงที่สุดในโมเดลนี้

การสนับสนุนจากองค์กร (Support from Organization: SP) มีค่าสัมประสิทธิ์ไม่มาตรฐาน (b) เท่ากับ 0.155 และมีค่า β เท่ากับ 0.127 โดยมีนัยสำคัญทางสถิติที่ระดับ $p = 0.010$ แสดงว่าเมื่อ Sp เพิ่มขึ้น 1 หน่วย จะทำให้ค่าเฉลี่ยของการรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (Perceived Usefulness: PU) เพิ่มขึ้น 0.155 หน่วย เมื่อควบคุมความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) ให้คงที่ แม้อิทธิพลจะน้อยกว่าความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) อย่างชัดเจน แต่ยังคงมีบทบาทเชิงบวกอย่างมีนัยสำคัญ สมการถดถอยเชิงเส้น (ไม่มาตรฐาน) สำหรับสมมติฐานที่ 1 สามารถเขียนได้ดังนี้

$$PU = 1.120 + 0.635(SA) + 0.155(SP) \quad (4-1)$$

4.4.2.2.1 การแปลความหมายเชิงสถิติ ความเหมาะสมของโมเดลโดยรวม ค่า $R = 0.681$ สะท้อนว่าตัวแปรความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) มีความสัมพันธ์รวมกับการรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (Perceived Usefulness: PU) ในระดับค่อนข้างสูง ขณะที่ค่า $R^2 = 0.464$ หมายความว่าโมเดลสามารถอธิบายความแปรปรวนของ การรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (Perceived Usefulness: PU) ได้ร้อยละ 46.4 ซึ่งถือว่าอยู่ในระดับที่น่าพึงพอใจสำหรับงานวิจัยด้านพฤติกรรมองค์กร ค่า $F = 107.00$ และ $p < .001$ บ่งชี้ว่าโมเดลโดยรวมมีนัยสำคัญทางสถิติ แสดงว่าการรวมกันของ ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) ช่วยเพิ่มความแม่นยำในการทำนาย PU อย่างมีนัยสำคัญเมื่อเทียบกับโมเดลที่ไม่มีตัวแปรอิสระ

4.4.2.2.2 อิทธิพลของความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) ค่าสัมประสิทธิ์ $b = 0.635$ ($p < .001$) แสดงถึงอิทธิพลเชิงบวกอย่างมีนัยสำคัญ กล่าวคือ เมื่อบุคลากรมีระดับความตระหนักรู้ด้านภัยคุกคามสูงขึ้น จะส่งผลให้การรับรู้มาตรฐานด้านความมั่นคงปลอดภัยมีประโยชน์เพิ่มสูงขึ้นอย่างชัดเจน ค่า β มาตรฐานที่สูงถึง 0.630 สะท้อนว่าความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) เป็นตัวแปรที่มีอิทธิพลมากที่สุดโมเดล ซึ่งชี้ให้เห็นถึงบทบาทสำคัญของปัจจัยด้านบุคลากรในการขับเคลื่อนการยอมรับและการรับรู้คุณค่าของมาตรการด้านความมั่นคงปลอดภัย

4.4.2.2.3 อิทธิพลของการสนับสนุนจากองค์กร (Support from Organization: SP) ค่าสัมประสิทธิ์ $b = 0.155$ ($p = 0.010$) บ่งชี้ว่า การสนับสนุนจากองค์กรมีอิทธิพลเชิงบวกต่อการรับรู้ประโยชน์ แม้ระดับอิทธิพลจะไม่สูงเท่ากับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) แต่ยังคงมีนัยสำคัญทางสถิติ ค่า $\beta = 0.127$ แสดงว่าการสนับสนุนจากองค์กร (Support from Organization: SP) เป็นปัจจัยเสริมที่ช่วยสนับสนุนให้บุคลากรมองเห็นคุณค่าและประโยชน์ของมาตรการ/มาตรฐานด้านความมั่นคงปลอดภัย โดยเฉพาะในบริบทที่องค์กรมีการจัดสรรทรัพยากร สนับสนุนเชิงนโยบาย และสร้างสภาพแวดล้อมที่เอื้อต่อการปฏิบัติตามมาตรฐาน

4.4.2.2.4 จากผลการวิเคราะห์ถดถอยพหุคูณ พบว่า ทั้งความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลเชิงบวกและมีนัยสำคัญทางสถิติต่อการรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (Perceived Usefulness: PU) ตามที่ตั้งสมมติฐานไว้

ดังนั้น สมมติฐานที่ 1 ได้รับการยอมรับ โดยสามารถสรุปได้ว่า บุคลากรที่มีความตระหนักรู้ด้านภัยคุกคามในระดับสูง และได้รับการสนับสนุนจากองค์กรอย่างเพียงพอ จะมีแนวโน้มรับรู้มาตรฐานและมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศมีประโยชน์ต่อการปฏิบัติงานมากขึ้น ซึ่งสอดคล้องกับกรอบแนวคิดด้านปัจจัยมนุษย์ (Human Factors) และการสนับสนุนเชิงองค์กรที่มีบทบาทสำคัญต่อความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ในระดับองค์กรอย่างมีนัยสำคัญ

4.4.2.2 สมมติฐานที่ 2: ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลเชิงบวกต่อความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) ด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร ผลการวิเคราะห์หาค่าถดถอยเชิงเส้นพหุคูณแสดงดังตารางที่ 4-14

ตารางที่ 4-14 ผลการวิเคราะห์หาค่าถดถอยพหุคูณของตัวแปรความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (SA) และการสนับสนุนจากองค์กร (SP) ที่มีต่อความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (CT)

รายการ	ค่าประมาณ	รายละเอียด
R	0.364	ความสัมพันธ์รวมระหว่าง SA, Sp กับ Ct
R ²	0.132	อธิบายความแปรปรวนของ Ct ได้ร้อยละ 13.2
Adjusted R ²	0.125	–
RMSE	0.687	ค่าคลาดเคลื่อนมาตรฐานของโมเดล
F (df1 = 2, df2 = 247)	18.80	ทดสอบความเหมาะสมของโมเดลโดยรวม
Sig. (p)	< .001	โมเดลมีนัยสำคัญทางสถิติที่ระดับ .001

จากตารางที่ 4-14 พบว่า ผลการวิเคราะห์หาค่าถดถอยเชิงเส้นพหุคูณพบว่า โมเดลที่ใช้ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) และ การสนับสนุนจากองค์กร (Support from Organization: SP) เป็นตัวแปรต้นในการทำนายความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) มีค่า R คือ 0.364 และค่า R² คือ 0.132 แสดงว่าตัวแปรอิสระทั้งสองสามารถอธิบายความแปรปรวนของการรับรู้ประโยชน์ได้ร้อยละ 13.20 แม้จะไม่สูงมาก แต่ก็มีนัยสำคัญทางสถิติ และถือว่ายอมรับได้สำหรับงานวิจัยด้านพฤติกรรมและการจัดการ

ค่า F คือ 18.80 และมีระดับนัยสำคัญทางสถิติที่ $p < .001$ แสดงว่าโมเดลถดถอยโดยรวมมีความเหมาะสม มีความแตกต่างอย่างมีนัยสำคัญจากโมเดลที่ไม่มีตัวแปรทำนาย (Null Model) กล่าวคือความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) เมื่อรวมกันแล้วมีศักยภาพในการทำนายความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) ได้อย่างมีนัยสำคัญทางสถิติ ค่าสัมประสิทธิ์ถดถอยของตัวแปรอิสระ แสดงดังตารางที่ 4-15

ตารางที่ 4-15 ค่าสัมประสิทธิ์ถดถอยของตัวแปรอิสระ ของตัวแปรความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (SA) และการสนับสนุนจากองค์กร (SP) ที่มีต่อความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (CT)

ตัวแปร	b (Estimate)	SE	t	p	β	ทิศทาง/นัยสำคัญ
Intercept	2.866	0.5708	5.02	< .001	–	มีนัยสำคัญ
SA	-0.361	0.0979	-3.69	< .001	-0.231	เชิงลบ มีนัยสำคัญ
Sp	0.687	0.1179	5.83	< .001	0.365	เชิงบวก มีนัยสำคัญ

จากตารางที่ 4-15 พบว่า ค่าสัมประสิทธิ์ถดถอยของตัวแปรอิสระ ของตัวแปรความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) ที่มีต่อความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT)

ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) มีค่าสัมประสิทธิ์ไม่มาตรฐาน (b) เท่ากับ -0.361 และมีค่า β เท่ากับ -0.231 โดยมีนัยสำคัญทางสถิติที่ระดับ $p < .001$ สะท้อนว่าความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) มีอิทธิพลเชิงลบต่อความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) อย่างมีนัยสำคัญ กล่าวคือ เมื่อระดับความตระหนักรู้ด้านภัยคุกคามเพิ่มขึ้น 1 หน่วย ระดับความสามารถในการควบคุมจะลดลง 0.361 หน่วย ภายใต้เงื่อนไขที่การสนับสนุนจากองค์กร (Support from Organization: SP) คงที่ ซึ่งเป็นผลลัพธ์ที่ไม่เป็นไปตามทิศทางที่ตั้งสมมติฐานไว้

การสนับสนุนจากองค์กร (Support from Organization: SP) มีค่าสัมประสิทธิ์ไม่มาตรฐาน (b) เท่ากับ 0.687 และ $\beta = 0.365$ โดยมีนัยสำคัญทางสถิติที่ระดับ $p < .001$ แสดงให้เห็นว่าเมื่อการสนับสนุนจากองค์กรเพิ่มขึ้น 1 หน่วย จะทำให้ความสามารถในการควบคุมเพิ่มขึ้น 0.687 หน่วย เมื่อควบคุมความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) ให้คงที่ และเป็นตัวแปรที่มีอิทธิพลสูงสุดในโมเดลนี้

สมการถดถอยเชิงเส้น (ไม่มาตรฐาน) สำหรับสมมติฐานที่ 2 สามารถเขียนได้ดังนี้

$$Ct = 2.866 - 0.361(SA) + 0.687(Sp) \quad (4-2)$$

4.4.2.2.1 การแปลความหมายเชิงสถิติ ความเหมาะสมของโมเดลโดยรวม ค่า $R^2 = 0.132$ แสดงว่า ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) สามารถร่วมกันอธิบายความแปรปรวนของความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) ได้ร้อยละ 13.20 แม้สัดส่วนการอธิบายจะอยู่ในระดับไม่สูงมาก แต่สำหรับงานวิจัยด้านพฤติกรรมและการจัดการองค์กร ซึ่งมีตัวแปรแวดล้อมและปัจจัยเชิงจิตวิทยาหลากหลาย ค่าดังกล่าวถือว่ายอมรับได้ในเชิงวิชาการ ผลการทดสอบค่า $F = 18.80$ และมีนัยสำคัญทางสถิติที่ระดับ $p < .001$ สะท้อนว่าโมเดลถดถอยโดยรวมมีความเหมาะสม และตัวแปรต้นทั้งสองเมื่อพิจารณาร่วมกันสามารถทำนายความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) ได้ดีกว่าโมเดลที่ไม่มีตัวแปรอิสระอย่างมีนัยสำคัญทางสถิติ

4.4.2.2.2 อิทธิพลของความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) ค่าสัมประสิทธิ์ถดถอยไม่มาตรฐาน (b) เท่ากับ -0.361 และมีนัยสำคัญทางสถิติที่ระดับ $p < .001$ แสดงว่า เมื่อระดับความตระหนักรู้ด้านภัยคุกคามเพิ่มขึ้น 1 หน่วย จะส่งผลให้ระดับความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) ลดลง 0.361 หน่วย ภายใต้เงื่อนไขที่การสนับสนุนจากองค์กร (Support from Organization: SP) คงที่ ค่า β มาตรฐาน เท่ากับ -0.231 สะท้อนอิทธิพลเชิงลบในระดับปานกลาง ผลลัพธ์ดังกล่าวไม่เป็นไปตามทิศทางเชิงบวกที่ตั้งสมมติฐานไว้ จึงไม่สามารถสนับสนุนสมมติฐานย่อยในส่วนของความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) ได้ในเชิงตีความ อาจสะท้อนปรากฏการณ์ที่ว่า เมื่อบุคลากรมีความตระหนักรู้ด้านภัยคุกคามสูงขึ้น ย่อมรับรู้ถึงความซับซ้อน ความเสี่ยง และข้อจำกัดเชิงเทคนิคมากขึ้น จึงประเมินว่าตนเองมีขีดความสามารถในการควบคุมสถานการณ์ได้จำกัดลง

4.4.2.2.3 อิทธิพลของการสนับสนุนจากองค์กร (Support from Organization: SP) ค่าสัมประสิทธิ์ถดถอยไม่มาตรฐาน (b) เท่ากับ 0.687 และมีนัยสำคัญทางสถิติที่ระดับ $p < .001$ แสดงว่า เมื่อระดับการสนับสนุนจากองค์กรเพิ่มขึ้น 1 หน่วย จะทำให้ค่าความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) เพิ่มขึ้น 0.687 หน่วย เมื่อควบคุม ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) ให้คงที่ ค่า $\beta = 0.365$ บ่งชี้ว่า การสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลเชิงบวกต่อความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) ในระดับปานกลางถึงค่อนข้างสูง และเป็นตัวแปรที่มีอิทธิพลมากที่สุดโมเดลนี้ สะท้อนว่าโครงสร้างพื้นฐาน นโยบาย ทรัพยากร และการสนับสนุนจากผู้บริหาร มีบทบาทสำคัญโดยตรงต่อความรู้สึกว่าบุคลากรสามารถควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศได้

4.4.2.2.4 จากผลการวิเคราะห์ถดถอยพหุคูณ พบว่า ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลต่อความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) อย่างมีนัยสำคัญทางสถิติ โดยเมื่อพิจารณาาร่วมกัน ตัวแปรทั้งสองสามารถอธิบายการเปลี่ยนแปลงของความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) ได้อย่างมีนัยสำคัญ

ดังนั้น สมมติฐานที่ 2 ได้รับการยอมรับ เนื่องจากผลการวิเคราะห์เชิงสถิติยืนยันว่า ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) ต่างมีอิทธิพลต่อความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) อย่างมีนัยสำคัญตามที่กำหนดไว้ในสมมติฐาน ข้อค้นพบดังกล่าวสะท้อนให้เห็นว่า การเสริมสร้างศักยภาพในการควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศจำเป็นต้องอาศัยทั้งมิติด้านบุคลากรและมิติด้านโครงสร้างองค์กรควบคู่กัน กล่าวคือ เมื่อบุคลากรมีความตระหนักรู้ต่อภัยคุกคามในระดับสูง และได้รับการสนับสนุนเชิงนโยบาย ทรัพยากร และระบบงานอย่างเหมาะสม ย่อมส่งผลให้เกิดความมั่นใจและความสามารถในการบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพมากยิ่งขึ้น จึงอาจกล่าวได้ว่า ความพร้อมด้านความมั่นคง

ปลอดภัยไซเบอร์ในระดับองค์กร เป็นผลลัพธ์ของการบูรณาการระหว่าง “ความรู้และความตระหนักรู้ของบุคลากร” กับ “กลไกสนับสนุนเชิงระบบขององค์กร” อย่างสมดุลและต่อเนื่อง

4.4.2.3 สมมติฐานที่ 3: ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลเชิงบวกต่อความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) ด้านความมั่นคงปลอดภัยสารสนเทศในองค์กร ผลการวิเคราะห์ถดถอยเชิงเส้นพหุคูณแสดงดังตารางที่ 4-16

ตารางที่ 4-16 ผลการวิเคราะห์ถดถอยพหุคูณของตัวแปร ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (SA) และการสนับสนุนจากองค์กร (SP) ที่มีต่อความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Dev)

รายการ	ค่าประมาณ	รายละเอียด
N	250	–
R	0.544	ความสัมพันธ์รวมระหว่าง SA, Sp กับ Dev
R ²	0.296	อธิบายความแปรปรวนของ Dev ได้ร้อยละ 29.6
Adjusted R ²	0.290	–
RMSE	1.380	ค่าคลาดเคลื่อนมาตรฐานของโมเดล
F (df1 = 2, df2 = 247)	51.90	ทดสอบความเหมาะสมของโมเดลโดยรวม
Sig. (p)	< .001	โมเดลมีนัยสำคัญทางสถิติ

จากตารางที่ 4-16 พบว่า ผลการวิเคราะห์ถดถอยเชิงเส้นพหุคูณพบว่า โมเดลมีค่า $R = 0.544$ แสดงถึงความสัมพันธ์เชิงบวกระดับปานกลางระหว่างตัวแปรอิสระ ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (SA) และการสนับสนุนจากองค์กร (SP) ที่มีต่อความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Dev) และมีค่า $R^2 = 0.296$ หมายความว่า ตัวแปรทั้งสองสามารถร่วมกันอธิบายความแปรปรวนของความต้องการพัฒนาระบบได้ร้อยละ 29.6 ซึ่งถือว่าอยู่ในระดับที่ยอมรับได้สำหรับงานวิจัยด้านพฤติกรรมองค์กร

ค่า Adjusted $R^2 = 0.290$ สะท้อนว่าเมื่อปรับค่าตามจำนวนตัวแปรแล้ว โมเดลยังคงมีความสามารถในการอธิบายข้อมูลในระดับใกล้เคียงกัน แสดงถึงความเสถียรของโมเดล ขณะที่ค่า $F(2, 247) = 51.90$ และมีนัยสำคัญทางสถิติที่ระดับ $p < .001$ แสดงว่า โมเดลถดถอยโดยรวมมีความเหมาะสม และสามารถทำนาย Dev ได้ดีกว่าโมเดลที่ไม่มีตัวแปรอิสระอย่างมีนัยสำคัญทางสถิติ

ค่าสัมประสิทธิ์ถดถอยของตัวแปรอิสระ แสดงดังตารางที่ 4-17

ตารางที่ 4-17 ค่าสัมประสิทธิ์ถดถอยของตัวแปรอิสระ ของตัวแปรความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (SA) และการสนับสนุนจากองค์กร (SP) ที่มีต่อความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Dev)

ตัวแปร	b (Estimate)	SE	t	p	β	ทิศทาง/นัยสำคัญ
Intercept	5.900	1.145	5.16	< .001	–	มีนัยสำคัญ
SA	1.190	0.196	6.06	< .001	0.341	เชิงบวก มีนัยสำคัญ
Sp	1.380	0.236	5.82	< .001	0.328	เชิงบวก มีนัยสำคัญ

จากตารางที่ 4-17 พบว่า ค่าสัมประสิทธิ์ถดถอยของตัวแปรอิสระ ของตัวแปร ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) มีค่าสัมประสิทธิ์ถดถอยไม่มาตรฐาน (b) เท่ากับ **1.190** (SE = 0.196, t = 6.06, p < .001, β = 0.341) แสดงว่า เมื่อ ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) เพิ่มขึ้น 1 หน่วย จะส่งผลให้ Dev เพิ่มขึ้น 1.190 หน่วย โดยมีอิทธิพลเชิงบวกและมีนัยสำคัญทางสถิติ

การสนับสนุนจากองค์กร (Support from Organization: SP) มีค่าสัมประสิทธิ์ถดถอยไม่มาตรฐาน (b) เท่ากับ **1.380** (SE = 0.236, t = 5.82, p < .001, β = 0.328) แสดงว่า เมื่อการสนับสนุนจากองค์กร (Support from Organization: SP) เพิ่มขึ้น 1 หน่วย จะส่งผลให้ ความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Dev) เพิ่มขึ้น 1.380 หน่วย อย่างมีนัยสำคัญทางสถิติ

สมการถดถอยเชิงเส้น (ไม่มาตรฐาน) สำหรับสมมติฐานที่ 3 สามารถเขียนได้ดังนี้

$$\text{Dev} = 5.90 + 1.19(\text{SA}) + 1.38(\text{Sp}) \quad (4-3)$$

4.4.2.3.1 การแปลความหมายเชิงสถิติ ความเหมาะสมของโมเดลโดยรวม ค่า $R^2 = 0.296$ แสดงว่า ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) สามารถร่วมกันอธิบายความแปรปรวนของความต้องการพัฒนาระบบ (Dev) ได้ร้อยละ 29.60 ซึ่งถือว่าอยู่ในระดับปานกลางและยอมรับได้สำหรับงานวิจัยด้านพฤติกรรมองค์กรและการจัดการระบบสารสนเทศ ผลการทดสอบค่า $F = 51.90$ และมีนัยสำคัญทางสถิติที่ระดับ $p < .001$ สะท้อนว่า โมเดลถดถอยโดยรวมมีความเหมาะสม และตัวแปรอิสระทั้งสองเมื่อพิจารณาาร่วมกันสามารถทำนายความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) ได้ดีกว่าโมเดลที่ไม่มีตัวแปรอิสระอย่างมีนัยสำคัญทางสถิติ พิจารณาร่วมกันสามารถทำนายความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) ได้ดีกว่าโมเดลที่ไม่มีตัวแปรอิสระอย่างมีนัยสำคัญทางสถิติ

4.4.2.3.2 อิทธิพลของความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) ค่าสัมประสิทธิ์ถดถอยไม่มาตรฐาน (b) เท่ากับ 1.190 และมีนัยสำคัญทางสถิติที่ระดับ $p < .001$ แสดงว่า เมื่อระดับความตระหนักรู้ด้านภัยคุกคามเพิ่มขึ้น 1 หน่วย จะส่งผลให้ระดับความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention:

Dev) เพิ่มขึ้น 1.190 หน่วย ภายใต้เงื่อนไขที่การสนับสนุนจากองค์กร (Support from Organization: SP) คงที่ ค่า β มาตรฐานเท่ากับ 0.341 สะท้อนอิทธิพลเชิงบวกในระดับปานกลาง ผลลัพธ์ดังกล่าวเป็นไปตามทิศทางของสมมติฐานที่ตั้งไว้ แสดงให้เห็นว่า บุคลากรที่มีความรู้และความเข้าใจต่อภัยคุกคามด้านไซเบอร์มากขึ้น จะยิ่งตระหนักถึงช่องโหว่ ข้อจำกัด และความจำเป็นในการยกระดับหรือพัฒนาระบบด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

4.4.2.3.3 อิทธิพลของการสนับสนุนจากองค์กร (Support from Organization: SP) ค่าสัมประสิทธิ์ถดถอยไม่มาตรฐาน (b) เท่ากับ 1.380 และมีนัยสำคัญทางสถิติที่ระดับ $p < .001$ แสดงว่า เมื่อระดับการสนับสนุนจากองค์กรเพิ่มขึ้น 1 หน่วย จะทำให้ค่าความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) เพิ่มขึ้น 1.380 หน่วย เมื่อควบคุมความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) ให้คงที่ ค่า $\beta = 0.328$ บ่งชี้ว่า Sp มีอิทธิพลเชิงบวกต่อความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) ในระดับใกล้เคียงกับ ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) สะท้อนว่า องค์กรที่มีนโยบายชัดเจน จัดสรรงบประมาณเพียงพอ และมีโครงสร้างพื้นฐานที่เหมาะสม จะช่วยกระตุ้นให้บุคลากรเกิดแรงผลักดันในการพัฒนาและยกระดับระบบความมั่นคงปลอดภัยสารสนเทศมากยิ่งขึ้น

4.4.2.3.4 จากผลการวิเคราะห์ถดถอยพหุคูณ พบว่า ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลเชิงบวกและมีนัยสำคัญทางสถิติต่อความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) โดยเมื่อพิจารณาาร่วมกัน ตัวแปรทั้งสองสามารถอธิบายการเปลี่ยนแปลงของความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) ได้อย่างมีนัยสำคัญ

ดังนั้น สมมติฐานที่ 3 ได้รับการยอมรับ เนื่องจากผลการวิเคราะห์เชิงสถิติยืนยันว่า ทั้ง ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) และ และการสนับสนุนจากองค์กร (Support from Organization: SP) ต่างมีอิทธิพลเชิงบวกต่อความต้องการพัฒนาระบบตามทิศทางที่กำหนดไว้ในสมมติฐาน ข้อค้นพบดังกล่าวสะท้อนให้เห็นว่า การยกระดับและพัฒนาระบบด้านความมั่นคงปลอดภัยสารสนเทศในองค์กร มิได้เกิดจากแรงผลักดันเชิงนโยบายเพียงอย่างเดียว หากแต่ต้องอาศัยความตระหนักรู้ของบุคลากรควบคู่กับการสนับสนุนเชิงโครงสร้างอย่างเป็นระบบ กล่าวคือ เมื่อบุคลากรรับรู้ถึงความเสี่ยงอย่างชัดเจน และองค์กรมีทรัพยากรพร้อมสนับสนุน ย่อมก่อให้เกิดพลังขับเคลื่อนในการพัฒนาระบบอย่างต่อเนื่องและยั่งยืน จึงอาจกล่าวได้ว่า ความต้องการพัฒนาระบบด้านความมั่นคงปลอดภัยไซเบอร์ เป็นผลลัพธ์ของการบูรณาการระหว่าง “มิติด้านบุคลากร” และ “มิติด้านการสนับสนุนเชิงองค์กร” ซึ่งทำงานประสานกันเพื่อเสริมสร้างความพร้อมขององค์กรในระยะยาว

4.4.3 สรุปภาพรวมผลการทดสอบสมมติฐาน

เพื่อให้เห็นภาพรวมของผลการวิเคราะห์สมมติฐานอย่างเป็นระบบ ผู้วิจัยได้สรุปผลการทดสอบสมมติฐานทั้งหมดไว้ในตารางที่ 4-18 โดยพิจารณาทั้งความเหมาะสมของโมเดล (R^2) ทิศทางความสัมพันธ์ และนัยสำคัญทางสถิติของตัวแปรที่ศึกษา

ตารางที่ 4-18 สรุปผลการทดสอบสมมติฐานโดยรวม

สมมติฐาน	ความสัมพันธ์ที่ทดสอบ	ผลเชิงสถิติ (สรุป)	ข้อสรุป
H1	SA, Sp $\rightarrow$ PU	โมเดลมี $R^2 = 0.464$, SA และ Sp มีอิทธิพลเชิงบวก มีนัยสำคัญ $p < .05$	ยอมรับสมมติฐาน
H2	SA, Sp $\rightarrow$ Ct	โมเดลมี $R^2 = 0.132$, Sp มีอิทธิพลเชิงบวกมีนัยสำคัญ แต่ SA มีอิทธิพลเชิงลบมีนัยสำคัญ	ยอมรับสมมติฐานบางส่วน
H3	SA, Sp $\rightarrow$ Dev	โมเดลมี $R^2 = 0.296$, SA และ Sp มีอิทธิพลเชิงบวก มีนัยสำคัญทั้งหมด	ยอมรับสมมติฐาน

จากตารางที่ 4- 18 พบว่า

ประการแรก ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) มีอิทธิพลเชิงบวกต่อการรับรู้ประโยชน์ในการนำมาตราฐานมาใช้ (Perceived Usefulness: PU) และความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) อย่างมีนัยสำคัญ สะท้อนให้เห็นว่า เมื่อบุคลากรมีความเข้าใจและตระหนักถึงภัยคุกคามมากขึ้น ย่อมมองเห็นคุณค่าและความจำเป็นของมาตรฐานความมั่นคงปลอดภัยสารสนเทศมากขึ้น และมีแนวโน้มสนับสนุนการพัฒนาระบบในอนาคต

อย่างไรก็ตาม ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) กลับมีอิทธิพลเชิงลบต่อความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) อย่างมีนัยสำคัญ ซึ่งเป็นข้อค้นพบที่น่าสนใจในเชิงวิชาการ กล่าวคือ บุคลากรที่มีระดับความตระหนักรู้สูง อาจรับรู้ถึงความซับซ้อนของภัยคุกคามและข้อจำกัดเชิงระบบมากขึ้น ส่งผลให้ประเมินความสามารถในการควบคุมของตนเองลดลง ปรากฏการณ์นี้สะท้อนมิติด้านจิตวิทยาการรับรู้ ความเสี่ยงที่ควรได้รับการศึกษาเพิ่มเติม

ประการที่สอง การสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลเชิงบวกและมีนัยสำคัญต่อทั้งสามตัวแปรตาม ได้แก่ การรับรู้ประโยชน์ในการนำมาตราฐานมาใช้ (Perceived Usefulness: PU) ความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) และความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) อย่างสม่ำเสมอในทุกโมเดล แสดงให้เห็นถึงบทบาทขององค์กรในฐานะ “กลไกขับเคลื่อนหลัก” ที่ช่วยเสริมสร้างการรับรู้คุณค่า ความเชื่อมั่นในศักยภาพการควบคุม และแรงผลักดันในการพัฒนาระบบด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นรูปธรรม

โดยภาพรวม ผลการวิเคราะห์สอดคล้องกับกรอบแนวคิดเชิงทฤษฎีที่เน้นการบูรณาการระหว่างมิติด้าน IT Security Readiness ซึ่งครอบคลุมนโยบาย โครงสร้างพื้นฐาน และทรัพยากร กับมิติด้าน Human Factors อันได้แก่ ความรู้ ความสามารถ และความตระหนักรู้ของบุคลากร ทั้งสองมิติทำงานร่วมกันในการยกระดับระดับการรับรู้มาตรฐาน และเสริมสร้างความพร้อมในการบริหารจัดการตามมาตรฐานความมั่นคงปลอดภัยขององค์กรอย่างยั่งยืน

กล่าวโดยสรุป งานวิจัยนี้ชี้ให้เห็นอย่างชัดเจนว่า ความสำเร็จในการยกระดับความมั่นคงปลอดภัยไซเบอร์มิได้เกิดจากปัจจัยด้านใดด้านหนึ่งเพียงลำพัง หากแต่เกิดจากการผสมผสานพลังระหว่าง “บุคลากรที่มีความตระหนักรู้” และ “องค์กรที่มีระบบสนับสนุนเข้มแข็ง” อย่างสมดุลและต่อเนื่องในระยะยาว



บทที่ 5

สรุปผล อภิปรายผล และข้อเสนอแนะ

การวิจัยเรื่อง “แนวทางพัฒนาการออกแบบเทคโนโลยีความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล เพื่อสอดคล้องกับมาตรฐาน HAIT Plus และ ISO/IEC 27001:2022” มีเป้าหมายสำคัญ 2 ประการ ได้แก่ (1) ศึกษาการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ของผู้บริหารโรงพยาบาลหลายสาขางาน และ (2) วิเคราะห์ปัจจัยที่มีอิทธิพลต่อการรับรู้มาตรฐานดังกล่าวตามแนวทาง HAIT Plus และ ISO/IEC 27001:2022 ทั้งนี้ งานวิจัยกำหนดขอบเขตพื้นที่เป็นโรงพยาบาลธรรมศาสตร์เฉลิมพระเกียรติ และใช้กลุ่มตัวอย่างจำนวน 250 คน โดยบทที่ 4 ได้นำเสนอผลการวิเคราะห์ข้อมูลเชิงพรรณนา การวิเคราะห์องค์ประกอบเชิงสำรวจ (EFA) และการทดสอบสมมติฐานด้วยการถดถอยเชิงเส้นพหุคูณ

- 5.1 สรุปผล
- 5.2 อภิปรายผลการวิจัย
- 5.3 ข้อเสนอแนะและแนวทางการพัฒนาต่อไป

5.1 สรุปผล

จากการดำเนินการวิจัยเรื่องการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ของผู้บริหารและบุคลากรโรงพยาบาล ผู้วิจัยสามารถสรุปผลการวิจัยตามวัตถุประสงค์ได้อย่างเป็นระบบ ดังนี้

5.1.1 วัตถุประสงค์ที่ 1 เพื่อศึกษาการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ของผู้บริหารโรงพยาบาล ผลการวิเคราะห์ระดับการรับรู้โดยรวม พบว่า “การรับรู้ด้านความพร้อมความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ (IT Security Readiness)” อยู่ในระดับ มาก โดยมีค่าเฉลี่ยรวม 3.85 และส่วนเบี่ยงเบนมาตรฐาน 0.78 สะท้อนว่ากลุ่มตัวอย่างโดยภาพรวมมีทักษะ/การรับรู้เชิงบวกต่อสภาพความพร้อมด้านความมั่นคงปลอดภัยในองค์กรโรงพยาบาล ซึ่งเป็น “ฐานรองรับ” ที่เอื้อต่อการยกระดับให้สอดคล้องกับ HAIT Plus และ ISO/IEC 27001:2022 ในเชิงระบบต่อไป

นอกจากนี้ เมื่อพิจารณาระดับการรับรู้ในมิติ “Human FaCTors” พบว่าอยู่ในระดับ มาก เช่นกัน (ค่าเฉลี่ยรวม 3.90, SD 0.74) โดยหากแยกรายมิติย่อย พบว่า

5.1.1.1 ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) ค่าเฉลี่ย 4.12 หรืออยู่ในระดับมาก

5.1.1.2 การสนับสนุนจากองค์กร (Support from Organization: SP) ค่าเฉลี่ย 3.94 หรืออยู่ในระดับมาก

5.1.1.3 การรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (Perceived Usefulness: PU) ค่าเฉลี่ย 3.77 หรืออยู่ในระดับมาก

5.1.1.4 ความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) ค่าเฉลี่ย 3.73 หรืออยู่ในระดับมาก

5.1.1.5 ความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) ค่าเฉลี่ย 3.92 หรืออยู่ในระดับมาก

ผลดังกล่าวสะท้อน “ภาวะพร้อมเชิงพฤติกรรมและการจัดการ” ของบุคลากร/ผู้บริหารในองค์กร กล่าวคือ มีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) สูง และมีความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) สูง ซึ่งตามตรรกะการกำกับดูแลความมั่นคงปลอดภัยแบบดั้งเดิม นี่คือสัญญาณเชิงบวกว่าองค์กร “เริ่มมองเห็นความเสี่ยง” และ “อยากยับยั้ง” ไม่ใช่แค่ทำเพราะถูกบังคับ

5.1.2 วัตถุประสงค์ที่ 2: เพื่อวิเคราะห์ปัจจัยที่มีอิทธิพลต่อการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ตามแนวทาง HAIT Plus และ ISO/IEC 27001:2022 งานวิจัยทดสอบสมมติฐานด้วยการถดถอยเชิงเส้นพหุคูณ (Multiple Linear Regression) โดยสรุปผลภาพรวมของสมมติฐานได้ดังนี้

5.1.3 สรุปผลการทดสอบสมมติฐาน

5.1.3.1 สมมติฐานที่ 1: ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลต่อการรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (Perceived Usefulness: PU) ผลการวิเคราะห์ถดถอยเชิงเส้นพหุคูณพบว่า แบบจำลองมีค่าสัมประสิทธิ์การกำหนด (R^2) เท่ากับ 0.464 แสดงว่าสามารถอธิบายความแปรปรวนของการรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (Perceived Usefulness: PU) ได้ร้อยละ 46.4 และแบบจำลองโดยรวมมีนัยสำคัญทางสถิติ ($F = 107.00, p < .001$) เมื่อพิจารณาเป็นรายตัวแปร พบว่า ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) มีอิทธิพลเชิงบวกต่อการรับรู้ประโยชน์อย่างมีนัยสำคัญทางสถิติ ($b = 0.635, \beta = 0.630, p < .001$) และการสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลเชิงบวกต่อการรับรู้ประโยชน์อย่างมีนัยสำคัญเช่นเดียวกัน ($b = 0.155, \beta = 0.127, p = 0.010$) กล่าวโดยสรุปเมื่อบุคลากรมีระดับความตระหนักรู้ต่อภัยคุกคามเพิ่มสูงขึ้น และได้รับการสนับสนุนจากองค์กรมากขึ้น ย่อมส่งผลให้ระดับการรับรู้ประโยชน์ของการยกระดับความมั่นคงปลอดภัยทางไซเบอร์เพิ่มสูงขึ้นอย่างมีนัยสำคัญ ดังนั้นจึงยอมรับสมมติฐานที่ 1

5.1.3.2 สมมติฐานที่ 2: ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลต่อความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) ผลการวิเคราะห์พบว่า แบบจำลองมีค่า R^2 เท่ากับ 0.132 และมีนัยสำคัญโดยรวมทางสถิติ ($F = 18.80, p < .001$) เมื่อพิจารณาเป็นรายตัวแปร พบว่า ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) มีอิทธิพลเชิงลบต่อความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) อย่างมีนัยสำคัญทางสถิติ ($b = -0.361, \beta = -0.231, p < .001$) ในขณะที่การสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลเชิงบวกต่อความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) อย่างมีนัยสำคัญ ($b = 0.687, \beta = 0.365, p < .001$) ผลการวิจัยสะท้อนให้เห็นว่า แม้การสนับสนุนจากองค์กรจะช่วยเสริมสร้างความสามารถในการควบคุมตามที่ตั้งสมมติฐานไว้ แต่ความตระหนักรู้ต่อภัยคุกคามที่เพิ่มสูงขึ้นกลับสัมพันธ์กับการประเมินความสามารถในการควบคุมที่ลดลงอย่างมีนัยสำคัญ ดังนั้น สมมติฐานที่ 2 จึงได้รับการยอมรับเพียงบางส่วน

5.1.3.3 สมมติฐานที่ 3: ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลต่อความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) ผลการวิเคราะห์พบว่า โมเดลมีค่า $R^2 = 0.296$ และมีนัยสำคัญโดยรวม ($F = 51.90$, $p < .001$) โดยรายตัวแปรพบว่า แบบจำลองมีค่า R^2 เท่ากับ 0.296 และมีนัยสำคัญโดยรวมทางสถิติ ($F = 51.90$, $p < .001$) เมื่อพิจารณาเป็นรายตัวแปร พบว่า ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) มีอิทธิพลเชิงบวกต่อความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) อย่างมีนัยสำคัญทางสถิติ ($b = 1.190$, $\beta = 0.341$, $p < .001$) และการสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลเชิงบวกต่อความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) อย่างมีนัยสำคัญเช่นกัน ($b = 1.380$, $\beta = 0.328$, $p < .001$)

กล่าวโดยสรุป การที่บุคลากรมีระดับความตระหนักรู้ต่อภัยคุกคามสูงขึ้น และได้รับการสนับสนุนจากองค์กรเพิ่มมากขึ้น จะส่งผลให้ความต้องการพัฒนาระบบความมั่นคงปลอดภัยทางไซเบอร์เพิ่มสูงขึ้นอย่างมีนัยสำคัญทางสถิติ ดังนั้นจึงยอมรับสมมติฐานที่ 3

5.1.4 สรุปผลการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) และข้อสังเกตสำคัญ

ผลการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ที่นำเสนอในบทที่ 4 แสดงให้เห็นว่า โครงสร้างองค์ประกอบของแบบวัดโดยรวมยังคงมีความสอดคล้องกับกรอบแนวคิดเชิงทฤษฎีที่กำหนดไว้ โดยเฉพาะในมิติความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) การสนับสนุนจากองค์กร (Support from Organization: SP) และความต้องการพัฒนาระบบ (Dev) ซึ่งมีจำนวนข้อคำถามที่เพียงพอ และมีค่าน้ำหนักองค์ประกอบ (factor loadings) อยู่ในเกณฑ์ที่เหมาะสม สะท้อนถึงความชัดเจนของโครงสร้างเชิงมิติและสอดคล้องภายในของตัวแปรแต่ละมิติ

อย่างไรก็ตาม ผลการวิเคราะห์ยังพบข้อสังเกตที่สำคัญ กล่าวคือ ในมิติการรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (Perceived Usefulness: PU) และความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) เหลือข้อคำถามเพียงมิติละ 1 ข้อในแบบจำลองสุดท้ายภายหลังการคัดกรอง ซึ่งอาจส่งผลกระทบต่อความครอบคลุมเชิงเนื้อหา (content coverage) และความมั่นคงเชิงจิตมิติของเครื่องมือวัด โดยเฉพาะในประเด็นความเที่ยงและความสามารถในการสะท้อนโครงสร้างเชิงนามธรรมของตัวแปรได้อย่างรอบด้าน

ดังนั้น แม้แบบจำลองโดยรวมจะยังคงมีความสอดคล้องกับกรอบแนวคิด แต่ข้อค้นพบดังกล่าวชี้ให้เห็นถึงความจำเป็นในการพัฒนาและขยายข้อคำถามในมิติ การรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (Perceived Usefulness: PU) และ ความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) ให้มีความหลากหลายและครอบคลุมมากยิ่งขึ้นในงานวิจัยครั้งต่อไป เพื่อเสริมสร้างความแข็งแกร่งเชิงโครงสร้าง (construct robustness) และยกระดับคุณภาพของเครื่องมือวัดในระยะยาว

5.2 อภิปรายผล

5.2.1 อภิปรายผลตามวัตถุประสงค์ที่ 1 ระดับการรับรู้มาตรฐานและความพร้อมด้านความมั่นคงปลอดภัย ผลการวิจัยพบว่า ระดับการรับรู้ด้าน IT Security Readiness ของผู้บริหารโรงพยาบาลอยู่ในระดับมาก หรือมีค่าเฉลี่ยเท่ากับ 3.85 และมีมิติด้าน Human Factors อยู่ในระดับมากเช่นกัน หรือมีค่าเฉลี่ยเท่ากับ 3.90 สะท้อนให้เห็นว่า โรงพยาบาลในฐานะองค์กรที่ให้บริการสาธารณสุขซึ่งมีลักษณะเป็นบริการวิกฤต (critical service) ย่อมเผชิญแรงกดดันจากความเสี่ยงด้านข้อมูลและข้อจำกัดเชิงนโยบายจำนวนมาก ส่งผลให้ผู้บริหารและผู้เกี่ยวข้องมีการรับรู้ถึงความจำเป็นของมาตรฐานและแนวทางการบริหารความมั่นคงปลอดภัยอย่างเป็นระบบในระดับสูง

เมื่อพิจารณารายมิติย่อย พบว่า ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness :SA) มีค่าเฉลี่ยสูงสุดที่ 4.12 บ่งชี้ว่าผู้บริหารและบุคลากรมีการรับรู้ถึงภัยคุกคามทางไซเบอร์อย่างชัดเจน อย่างไรก็ตาม การตระหนักรู้เพียงอย่างเดียวมิได้เพียงพอที่จะทำให้องค์กรมีความมั่นคงปลอดภัยเพิ่มขึ้น หากไม่ถูกแปรเปลี่ยนเป็นมาตรการเชิงระบบ กระบวนการทำงาน เทคโนโลยีที่เหมาะสม และการจัดสรรทรัพยากรตามหลักการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ในขณะเดียวกัน มิติความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) มีค่าเฉลี่ยอยู่ในระดับสูง 3.92 สะท้อนถึงแรงขับเคลื่อนในระดับนโยบายและการบริหาร กล่าวคือ องค์กรไม่ได้เพียงตระหนักถึงความเสี่ยง แต่ยังมีแนวโน้มพร้อมขับเคลื่อนการเปลี่ยนแปลงเชิงระบบ ผลดังกล่าวจึงถือเป็น “หน้าต่างโอกาสเชิงกลยุทธ์” สำหรับการยกระดับมาตรฐานความมั่นคงปลอดภัย โดยเฉพาะการบูรณาการแนวทาง HAIT Plus ในบริบทบริการสุขภาพ เข้ากับกรอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตาม ISO/IEC 27001:2022 อย่างเป็นระบบ

5.2.2 อภิปรายผลสมมติฐานที่ 2: อิทธิพลของความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) และ การสนับสนุนจากองค์กร (Support from Organization: SP) ต่อความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) ผลการวิเคราะห์พบว่า ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) มีอิทธิพลเชิงลบต่อความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) อย่างมีนัยสำคัญทางสถิติ ขณะที่การสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลเชิงบวกต่อความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) อย่างมีนัยสำคัญ ข้อค้นพบดังกล่าวสามารถอธิบายได้ในหลายมิติ ดังนี้

ประการแรก ในมุมมองเชิงพฤติกรรมองค์กร การที่ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) เพิ่มขึ้นอาจทำให้บุคลากรตระหนักถึงความซับซ้อน ความรุนแรง และความเปลี่ยนแปลงอย่างรวดเร็วของภัยคุกคามทางไซเบอร์ ส่งผลให้เกิดการประเมิณว่าการควบคุมหรือจัดการภัยคุกคามดังกล่าวเป็นเรื่องที่ยากลำบาก จึงสะท้อนออกมาในรูปของการลดลงของระดับความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) กล่าวอีกนัยหนึ่ง การรับรู้ความเสี่ยงที่เพิ่มขึ้นอาจทำให้ระดับความมั่นใจในการควบคุมลดลง โดยเฉพาะในบริบทที่ทรัพยากรหรือเครื่องมือสนับสนุนยังไม่เพียงพอ

ประการที่สอง หากการสร้างความรู้ความตระหนักรู้เน้นการสื่อสารความรุนแรงของภัยคุกคามโดยไม่ควบคู่กับแนวทางปฏิบัติที่ชัดเจนหรือกลไกสนับสนุนที่เป็นรูปธรรม อาจทำให้เกิดผลเชิงจิตวิทยาในลักษณะของความกังวลหรือความกลัวมากกว่าความรู้สึกรับรู้ควบคุมได้ ส่งผลให้ระดับความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) ลดลงได้ ประการที่สาม ในเชิงจิตมิติเครื่องมือวัดในมิติ ความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) เหลือข้อคำถามเพียงหนึ่งข้อในแบบจำลองสุดท้ายจากการวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis: EFA) ซึ่งอาจทำให้การสะท้อนแนวคิด “ความสามารถในการควบคุม” ครอบคลุมเพียงบางมุมมอง เช่น ความมั่นใจส่วนบุคคล มากกว่าความสามารถในการควบคุมเชิงระบบ จึงอาจทำให้ความสัมพันธ์กับ ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) ปรากฏในทิศทางลบได้ง่ายขึ้น

ในทางตรงกันข้าม การสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลเชิงบวกต่อความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) อย่างชัดเจน สอดคล้องกับหลักการบริหารความมั่นคงปลอดภัยสารสนเทศที่ระบุว่า ความสามารถในการควบคุมมิได้เป็นคุณลักษณะส่วนบุคคลเพียงลำพัง หากแต่เป็นผลลัพธ์ของระบบสนับสนุนที่เหมาะสม ได้แก่ นโยบายที่ชัดเจน กระบวนการตอบสนองเหตุการณ์ เครื่องมือทางเทคนิค การฝึกอบรม และการจัดสรรทรัพยากรที่เพียงพอ

ดังนั้น ข้อค้นพบนี้ชี้ให้เห็นว่า การยกระดับความตระหนักรู้ด้านภัยคุกคามควรดำเนินควบคู่กับการเสริมสร้างกลไกสนับสนุนเชิงระบบ มิฉะนั้น ระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) ที่สูงอาจไม่แปรผลเป็นความสามารถในการควบคุมที่สูงขึ้น แต่กลับส่งผลให้บุคลากรรู้สึกถึงความเสี่ยงอยู่เหนือการควบคุมของตนเอง

5.2.3 อภิปรายผลสมมติฐานที่ 3: อิทธิพลของความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) ต่อความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) ผลการวิเคราะห์พบว่า ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) และการสนับสนุนจากองค์กร (Support from Organization: SP) สามารถอธิบายความแปรปรวนของความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) ได้ร้อยละ 29.60 ($R^2 = 0.296$) และทั้งสองตัวแปรมีอิทธิพลเชิงบวกอย่างมีนัยสำคัญทางสถิติ ในเชิงการบริหารจัดการ สามารถตีความได้ว่า เมื่อบุคลากรมีการรับรู้ถึงภัยคุกคามอย่างชัดเจน และในขณะเดียวกันองค์กรมีระบบสนับสนุนที่เพียงพอ จะก่อให้เกิดแรงผลักดันภายในในการพัฒนาระบบความมั่นคงปลอดภัยให้มีความเข้มแข็งยิ่งขึ้น กล่าวได้ว่า ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) ทำหน้าที่เป็นแรงผลักดันจากการรับรู้ความเสี่ยง ขณะที่ SP ทำหน้าที่เป็นแรงสนับสนุนที่ทำให้การพัฒนาเป็นไปได้ในทางปฏิบัติ

นอกจากนี้ ค่าสัมประสิทธิ์เชิงถดถอยของการสนับสนุนจากองค์กร (Support from Organization: SP) ต่อ ความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) มีขนาดสูงกว่า ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) ในเชิงค่าสัมประสิทธิ์ดิบ (b) สะท้อนเชิงนโยบายว่า หากองค์กรต้องการ

ให้เกิดการพัฒนาระบบอย่างเป็นรูปธรรม จำเป็นต้องลงทุนและสนับสนุนเชิงโครงสร้างอย่างจริงจัง มีข้ออาศัยเพียงการสื่อสารเพื่อสร้างความตระหนักรู้เท่านั้น

5.3 ข้อเสนอแนะ

ข้อเสนอแนะจากการวิจัยครั้งนี้ แบ่งออกเป็น 3 ส่วน ได้แก่ (1) ข้อเสนอแนะเชิงปฏิบัติการ สำหรับโรงพยาบาลและผู้บริหาร (2) ข้อเสนอแนะเชิงนโยบาย/เชิงระบบ และ (3) ข้อเสนอแนะ สำหรับการวิจัยในอนาคต โดยมีรายละเอียดดังต่อไปนี้

5.3.1 ข้อเสนอแนะเชิงปฏิบัติการ (สำหรับโรงพยาบาล)

จากผลการวิจัยที่พบว่า การสนับสนุนจากองค์กร (Support from Organization: SP) มีอิทธิพลเชิงบวกอย่างมีนัยสำคัญต่อการรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (Perceived Usefulness: PU) ความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) และความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) อย่างสม่ำเสมอในทุกแบบจำลอง จึงสามารถสรุปเชิงปฏิบัติการได้ว่า “การสนับสนุนจากองค์กร” เป็นกลไกสำคัญในการขับเคลื่อนการยกระดับความมั่นคงปลอดภัยของโรงพยาบาลให้เกิดผลอย่างเป็นรูปธรรม ดังนั้น โรงพยาบาลควรดำเนินการดังต่อไปนี้

5.3.1.1 กำหนดการสนับสนุนจากองค์กรให้เป็นระบบที่ชัดเจนและตรวจสอบได้ การสนับสนุนจากองค์กรควรถูกกำหนดให้อยู่ในรูปของมาตรการเชิงโครงสร้างที่สามารถประเมินผลได้ ไม่ควรจำกัดอยู่เพียงการแสดงเจตนารมณ์เชิงนโยบาย โดยแนวทางที่เหมาะสม ได้แก่

5.3.1.1.1 การจัดสรรงบประมาณด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นหมวดหมู่ชัดเจน เช่น งบประมาณสำหรับการฝึกอบรมบุคลากร การตรวจประเมินภายในและภายนอก การพัฒนาแผนตอบสนองเหตุการณ์ (incident response) และการจัดหาเครื่องมือด้านเทคนิค

5.3.1.1.2 การกำหนดบทบาท หน้าที่ และความรับผิดชอบด้านความมั่นคงปลอดภัยอย่างชัดเจนในระดับองค์กร เช่น การกำหนดโครงสร้างความรับผิดชอบ (RACI) เพื่อให้เกิดความชัดเจนด้านการตัดสินใจ การกำกับดูแล และการปฏิบัติ

5.3.1.1.3 การจัดตั้งคณะกรรมการหรือคณะทำงานด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee) และเชื่อมโยงการดำเนินงานเข้ากับระบบบริหารคุณภาพของโรงพยาบาล เพื่อให้การกำกับดูแลมีความต่อเนื่องและบูรณาการในระดับองค์กร

ข้อเสนอแนะดังกล่าวมีพื้นฐานจากผลการวิจัยที่ชี้ให้เห็นว่า การสนับสนุนจากองค์กรเป็นปัจจัยสำคัญที่ช่วยยกระดับทั้งความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) และความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) อย่างมีนัยสำคัญ

5.3.1.2 ออกแบบการสร้างความรู้ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) ควบคู่กับแนวทางปฏิบัติที่ชัดเจนแม้ว่าระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) จะอยู่ในระดับสูง แต่ผลการวิจัยพบว่าความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) อาจสัมพันธ์เชิงลบกับความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) หากไม่มีระบบสนับสนุนที่เพียงพอ ดังนั้นการสร้างความรู้ความตระหนักรู้ควรออกแบบให้ควบคู่กับแนวทางปฏิบัติที่สามารถดำเนินการได้จริง โดยควรดำเนินการดังนี้

5.3.1.2.1 การสื่อสารความเสี่ยงความมาพร้อมขั้นตอนการปฏิบัติที่ชัดเจน (actionable guidance) เพื่อให้บุคลากรสามารถนำไปใช้ได้ทันที

5.3.1.2.2 มี playbook สั้น ๆ ให้ทำตามได้จริง (เช่น วิธีรับมือ phishing, ransomware, data leakage)

5.3.1.2.3 การจัดฝึกซ้อมสถานการณ์จำลอง (tabletop exercise) อย่างสม่ำเสมอ เพื่อเสริมสร้างความสามารถในการควบคุมจากประสบการณ์ตรง มีข้ออาศัยเพียงการรับรู้เชิงทฤษฎี

5.3.1.3 ดำเนินโครงการระยะสั้นที่เห็นผลชัดเจน (Quick Wins) เนื่องจากแบบจำลองในสมมติฐานที่ 1 สามารถอธิบายการรับรู้ประโยชน์ในการนำมาตรฐานมาใช้ (Perceived Usefulness: PU) ได้ในระดับค่อนข้างสูง ($R^2 = 0.464$) โรงพยาบาลจึงควรดำเนินโครงการที่ทำให้ “ประโยชน์” ของมาตรการด้านความมั่นคงปลอดภัยปรากฏอย่างชัดเจนในระยะสั้น เช่น

5.3.1.3.1 การทบทวนและกำหนดนโยบายการจัดชั้นความลับของข้อมูลผู้ป่วยอย่างเป็นระบบ

5.3.1.3.2 การพัฒนาระบบควบคุมสิทธิ์การเข้าถึง (Access Control) และกำหนดกระบวนการทบทวนสิทธิ์อย่างสม่ำเสมอ

5.3.1.3.3 การจัดทำระบบสำรองข้อมูล (backup) และการทดสอบกระบวนการกู้คืนข้อมูล (restore drill) อย่างต่อเนื่อง

การดำเนินการดังกล่าวจะช่วยให้บุคลากรมองเห็นคุณค่าของมาตรการด้านความมั่นคงปลอดภัยอย่างเป็นรูปธรรม ซึ่งจะส่งผลต่อความต้องการพัฒนาระบบในระยะต่อไปโดยธรรมชาติ

5.3.2 ข้อเสนอแนะเชิงนโยบาย/เชิงระบบ

5.3.2.1 จัดทำแผนแม่บทด้านความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาล จากผลการวิจัยที่พบว่าผู้บริหารมีระดับการรับรู้และทัศนคติเชิงบวกต่อความมั่นคงปลอดภัยในระดับมาก โรงพยาบาลจึงมีความพร้อมในการยกระดับจากการดำเนินกิจกรรมเฉพาะด้านไปสู่การจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) อย่างครบวงจร โดยควรกำหนดแผนแม่บทที่บูรณาการแนวทาง HAIT Plus เข้ากับกรอบ ISO/IEC 27001:2022 อย่างเป็นขั้นตอน ได้แก่

5.3.2.1.1 เป้าหมายระยะสั้น (1 ปี): การประเมินสถานะปัจจุบัน (baseline assessment) และการดำเนินมาตรการพื้นฐานที่จำเป็น

5.3.2.1.2 ระยะกลาง (2–3 ปี): การพัฒนาระบบตรวจประเมินภายใน (internal audit) และการยกระดับวุฒิภาวะ (maturity level)

5.3.2.1.3 ระยะยาว (3–5 ปี): การเตรียมความพร้อมสู่การรับรองมาตรฐาน หรือการประเมินความสอดคล้องอย่างยั่งยืน

5.3.2.2 กำหนดตัวชี้วัดระดับองค์กรที่สะท้อนความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) และความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) เนื่องจากแบบจำลองที่อธิบายความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) มีค่า R^2 ค่อนข้างต่ำ (0.132) สะท้อนว่า ความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) อาจได้รับอิทธิพลจากปัจจัยอื่นเพิ่มเติม องค์กรจึงควรกำหนดตัวชี้วัดเชิงประสิทธิผลที่สะท้อนความสามารถในการควบคุมอย่างเป็นรูปธรรม เช่น

5.3.2.2.1 ระยะเวลาเฉลี่ยในการตรวจพบและตอบสนองต่อเหตุการณ์ (Mean Time to Detect: MTTD และ Mean Time to Respond: MTTR)

5.3.2.2.2 อัตราการปฏิบัติตามกระบวนการทบทวนสิทธิ์การเข้าถึงข้อมูล

5.3.2.2.3 อัตราการผ่านการทดสอบหรือฝึกซ้อมแผนตอบสนองเหตุการณ์

การกำหนดตัวชี้วัดดังกล่าวจะช่วยให้ความสามารถในการควบคุมไม่เพียงการรับรู้เชิงความรู้สึก แต่เป็นศักยภาพที่สามารถวัด ประเมิน และพัฒนาได้อย่างต่อเนื่องในระดับองค์กร.

5.3.3 ข้อเสนอแนะสำหรับงานวิจัยในอนาคต

5.3.3.1 ปรับปรุงเครื่องมือวัดมิติการรับรู้ประโยชน์ในการนำมาตราฐานมาใช้ (Perceived Usefulness: PU) และความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) ให้มีหลายข้อคำถาม เนื่องจากผลการวิเคราะห์องค์ประกอบ ระบุว่า การรับรู้ประโยชน์ในการนำมาตราฐานมาใช้ (Perceived Usefulness: PU) และความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) เหลือเพียง 1 ข้อ งานวิจัยถัดไปควรพัฒนาเครื่องมือวัดให้ครอบคลุม (เพิ่มจำนวนข้อ ตรวจสอบความเที่ยง/ความตรง) เพื่อยืนยันความเสถียรของโครงสร้างตัวแปร

5.3.3.2 เพิ่มตัวแปรระดับองค์กร/โครงสร้างพื้นฐาน เพราะ ความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) มี R^2 ต่ำ อาจมีตัวแปรแฝงอื่น เช่น วัฒนธรรมองค์กร ภาวะผู้นำ ความพร้อมด้านงบประมาณจริง ระดับความซับซ้อนของระบบ/การพึ่งพา vendor ซึ่งควรนำเข้ามาทดสอบเพื่อเพิ่มพลังอธิบาย

5.3.3.3 ขยายกลุ่มตัวอย่างหลายโรงพยาบาล/หลายระดับบริการ เพื่อเปรียบเทียบโรงพยาบาลขนาดต่างกัน (ศูนย์/ทั่วไป/ชุมชน) ว่าความสัมพันธ์ของ ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ (Security Awareness: SA) การสนับสนุนจากองค์กร (Support from Organization: SP) การรับรู้ประโยชน์ในการนำมาตราฐานมาใช้ (Perceived Usefulness: PU) ความสามารถในการควบคุมภัยคุกคามทางไซเบอร์ (Control of Threats: CT) และความต้องการพัฒนาระบบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Development Intention: Dev) แตกต่างกันหรือไม่ และเพิ่มความสามารถในการสรุปอ้างอิงเชิงนโยบาย

บรรณานุกรม

ภาษาไทย

จุฬามาศ อยู่เจริญ และกิตติศักดิ์ แก้วบุตรดี. (2566). ความสำคัญของมาตรฐาน ISO/IEC 27001 และระบบบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศในโรงพยาบาล.

วารสาร Mahidol R2R e-Journal. 10(1), 16-28.

เบญจมาศ ปรีชาคุณ, ฤชดา โมเหล็ก, ดารารัตน์ ชูวงศ์อินทร์, เพ็ญพัทธ์ กองเมือง และมาริษา สมบัติบุรณ์. (2564). การพยาบาลในยุคเทคโนโลยีแห่งข้อมูล. วารสารราชวิทยาลัย จุฬารักษ์. 3(1), 19-39.

ราชกิจจานุเบกษา. (2566). ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566. 190, 39-40.

วนิดา อินทรอำนวย. (2560). การประกอบกิจการสถานพยาบาลตามพระราชบัญญัติ

สถานพยาบาล พ.ศ.2541. เข้าถึงได้จาก :

https://www.parliament.go.th/ewtadmin/ewt/elaw_parcy/ewt_dl_link.php?nid=1529. (วันที่ค้น ข้อมูล 26 สิงหาคม 2567)

วิไล ฤทธิเดช (2565). ความรู้ ความตระหนัก และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ ของบุคลากรสาธารณสุขในประเทศไทย: กรณีศึกษาโรงพยาบาลพุทธโสธร. วิทยานิพนธ์เภสัชศาสตร์มหาบัณฑิต สาขาวิชาสารสนเทศทางสุขภาพ. บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร.

ศิริลักษณ์ ดีเลิศไพบูลย์. (2565). การพัฒนาความรอบรู้ด้านดิจิทัลของพยาบาลวิชาชีพ. วารสาร วชิรสารการพยาบาล. 25(1), 70-79.

สมศิริ พันธุ์ศักดิ์ศิริ และเสาวนีย์ สมันต์ตรีพร. (2565). ประสิทธิผลของการจัดการความปลอดภัยระบบสารสนเทศ โรงพยาบาลสระบุรี. วารสารสหวิทยาการมนุษยศาสตร์ และสังคมศาสตร์. 6(2), 1046-1066.

สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และสมาคมเวชสารสนเทศไทย. (2567). แนวทางการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับโรงพยาบาลของรัฐ. เข้าถึงได้จาก https://tmi.or.th/wp-content/uploads/2023/12/HAIT_Plus_Guideline.pdf. (วันที่สืบค้น 20 กันยายน 2568)

สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (2566). คำแนะนำ เรื่อง
แนวทางปฏิบัติในการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
และการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานโครงสร้าง
พื้นฐานสำคัญทางสารสนเทศ. เข้าถึงได้จาก
[https://drive.ncsa.or.th/s/GXEamHQin9JaWZB?dir=/](https://drive.ncsa.or.th/s/GXEamHQin9JaWZB?dir=/&editing=false&openfile=true)
&editing=false&openfile=true. (วันที่สืบค้น 2 สิงหาคม 2568)

อริป แทนรัตนกุล. (2567) การสร้างวัฒนธรรมไซเบอร์เชิงบวก สำหรับนักศึกษาระดับปริญญา
ตรี. วารสารกองทุนพัฒนาสื่อปลอดภัยและสร้างสรรค์. 3(1), 80-105.

อนันต์ ชูยิ่งสกุลทิพย์. (2562). ระบบการพัฒนาสมรรถนะด้านเทคโนโลยีสารสนเทศและการ
สื่อสารเพื่อความมั่นคงปลอดภัยของสารสนเทศ. ดุษฎีนิพนธ์ปรัชญาดุษฎีบัณฑิต,
สาขาวิชาเทคโนโลยีการศึกษา, คณะศึกษาศาสตร์, มหาวิทยาลัยบูรพา.

เอชิสโปรเฟสชันแนล เซ็นต์เตอร์. (2566). องค์ประกอบของความมั่นคงปลอดภัยสารสนเทศ
(Elements of Information Security). เข้าถึงได้จาก [https://www.acisonline.net](https://www.acisonline.net/?p=8647)
/?p=8647. (วันที่สืบค้น 26 สิงหาคม 2567)

ภาษาอังกฤษ

Bulgurcu, B., Cavusoglu, H., & Benbasat, I.. (2010). Information security policy
compliance: An empirical study of rationality-based beliefs and information
security awareness. MIS Quarterly, 34(3), 523–548.

Dobski Pawel. (2024). Information Security Management in the Operations of
Healthcare Entities. Scientific Papers of Silesian University of Technology,
Organization and Management. 192, 179-198.

DiMaggio, P. J., & Powell, W. W.. (1983). The iron cage revisited: Institutional
isomorphism and collective rationality in organizational fields. American
Sociological Review, 48(2), 147–160.

Elham Abdullah and Al-Qarni. (2023). Cybersecurity in Healthcare: A Review of Recent
Attacks and Mitigation Strategies. International Journal of Advanced Computer
Science and Applications. 14(5), 135-140.

- Herath, T., & Rao, H. R.. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154–165.
- Ifinedo, P.. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83–95.
- International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.
- International Organization for Standardization. (2022). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. ISO.
- Kamalanathan Kandasamy, Sethuraman Srinivas and Krishnashree Achuthan. (2022). Digital Healthcare – Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risk, NIST perspectives, and Recommendations. *IEEE Access Open Access Journal*. 10, 12345-12364.
- National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity. Department of Commerce.
- National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5). U.S. Department of Commerce.
- Siponen, M., Pahlila, S., & Mahmood, M. A.. (2010). Compliance with information security policies: An empirical investigation. *Computer*, 43(2), 64–71.
- World Economic Forum. (2023). Healthcare cyber attacks are on the rise: Here's why zero trust will prevent care disruptions. เข้าถึงได้จาก <https://www.weforum.org/agenda/2023/05/cyber-attacks-on-healthcare-rise-zero-trust/>. (วันที่สืบค้น 25 สิงหาคม 2567)



แบบสอบถามการวิเคราะห์ปัจจัยการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์
สำหรับโรงพยาบาล
จัดทำโดย นางสาวผ่องศรี ประสมบุญ

นักศึกษาหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาระบบสารสนเทศเพื่อการจัดการ
คณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล มหาวิทยาลัยพระจอมเกล้าพระนครเหนือ

คำอธิบาย

แบบสอบถามนี้มีความประสงค์ขอเก็บรวบรวมข้อมูลของท่านผู้ตอบแบบสอบถามเพื่อนำไป
“วิเคราะห์ปัจจัยการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล” ประกอบไป
ด้วย 2 ส่วนคือ

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

ส่วนที่ 2 ปัจจัยการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล

ปัจจัยด้านความพร้อมความมั่นคงเทคโนโลยีสารสนเทศ

ปัจจัยด้านบุคลากร

ปัจจัยด้านการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์

ปัจจัยด้านบริหารจัดการตามมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์

โดยขอความอนุเคราะห์ท่านตอบแบบสอบถามดังกล่าวเพื่อนำไปวิเคราะห์ข้อมูลให้ตอบ
วัตถุประสงค์เพื่อการศึกษาต่อไป

หากท่านมีความประสงค์ต้องการตอบแบบสอบถามออนไลน์นี้โปรดให้การยินยอมเก็บข้อมูล
เพื่อการศึกษา

☐ ยินยอม

☐ ไม่ยินยอม

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

1. เพศ

☐

ชาย

☐

ไม่ต้องการระบุ

☐

หญิง

2. อายุ

☐

18 - 30 ปี

☐

51 - 60 ปี

☐

31 - 40 ปี

☐

60 - 70 ปี

☐

41 - 50 ปี

☐

มากกว่า 70 ปี

3. ระดับการศึกษา

☐

ปริญญาเอก

☐

มัธยมศึกษาตอนปลาย/อนุปริญญา

☐

ปริญญาโท

☐

มัธยมศึกษาตอนต้น

☐

ปริญญาตรี

☐

ต่ำกว่ามัธยมศึกษา

4. สังกัดฝ่าย

☐

สังกัดฝ่าย

☐

ฝ่ายเทคโนโลยีสารสนเทศ

☐

ฝ่ายการแพทย์/ห้องปฏิบัติการ

☐

ฝ่ายการเงิน/ธุรการ

☐

ฝ่ายการพยาบาล

☐

ฝ่ายเภสัชกรรม

☐

ฝ่ายคุณภาพ

5. ประสบการณ์ทำงาน/ความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์

☐

1-3 ปี

☐

7 ปีขึ้นไป

☐

4-6 ปี

☐

ไม่มีประสบการณ์



ส่วนที่ 2 ปัจจัยการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล

คำชี้แจง โปรดอ่านข้อความต่อไปนี้ แล้วเลือกระดับความคิดเห็นที่ตรงกับความเป็นจริงหรือ โดยให้คะแนนแบบมาตรวัดประมาณค่า 5 ระดับ (5 - point Likert Scale) ดังความหมายต่อไปนี้

ระดับ 5 หมายถึง เห็นด้วยอย่างยิ่ง

ระดับ 4 หมายถึง เห็นด้วย

ระดับ 3 หมายถึง เฉย ๆ

ระดับ 2 หมายถึง ไม่เห็นด้วย

ระดับ 1 หมายถึง ไม่เห็นด้วยอย่างยิ่ง

กรุณาเลือกเพียงคำตอบเดียวที่ตรงกับความคิดเห็นของท่านในแต่ละข้อ

1. ปัจจัยด้านความพร้อมความมั่นคงเทคโนโลยีสารสนเทศ (IT Security Readiness)

หมายถึง ระดับความพร้อมของโรงพยาบาลในด้านโครงสร้างพื้นฐาน ระบบงาน นโยบาย และทรัพยากรที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ โดยครอบคลุมทั้งมาตรการเชิงเทคนิคและเชิงบริหารจัดการ ปัจจัยนี้สะท้อนศักยภาพขององค์กรในการป้องกัน ตรวจสอบ และตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสม

ลำดับ	รายการคำถาม	ระดับความคิดเห็นของท่าน				
		ไม่เห็นด้วยอย่างยิ่ง	ไม่เห็นด้วย	เฉย ๆ	เห็นด้วย	เห็นด้วยอย่างยิ่ง
1	นโยบายและระเบียบปฏิบัติ					
2	โครงสร้างพื้นฐานเทคโนโลยี					
3	ทรัพยากรและการสนับสนุน					

2. ปัจจัยด้านบุคลากร (Human Factors) หมายถึง ความสามารถ ความรู้ ความเข้าใจ และพฤติกรรมของบุคลากรที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งถือเป็นองค์ประกอบสำคัญของระบบความมั่นคงปลอดภัย เนื่องจากบุคลากรเป็นทั้งผู้ใช้งานระบบและอาจเป็นจุดเสี่ยงของการเกิดภัยคุกคาม

ลำดับ	รายการคำถาม	ระดับความคิดเห็นของท่าน				
		ไม่เห็นด้วยอย่างยิ่ง	ไม่เห็นด้วย	เฉยๆ	เห็นด้วย	เห็นด้วยอย่างยิ่ง
1	สมรรถนะและความรู้					
2	ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์					

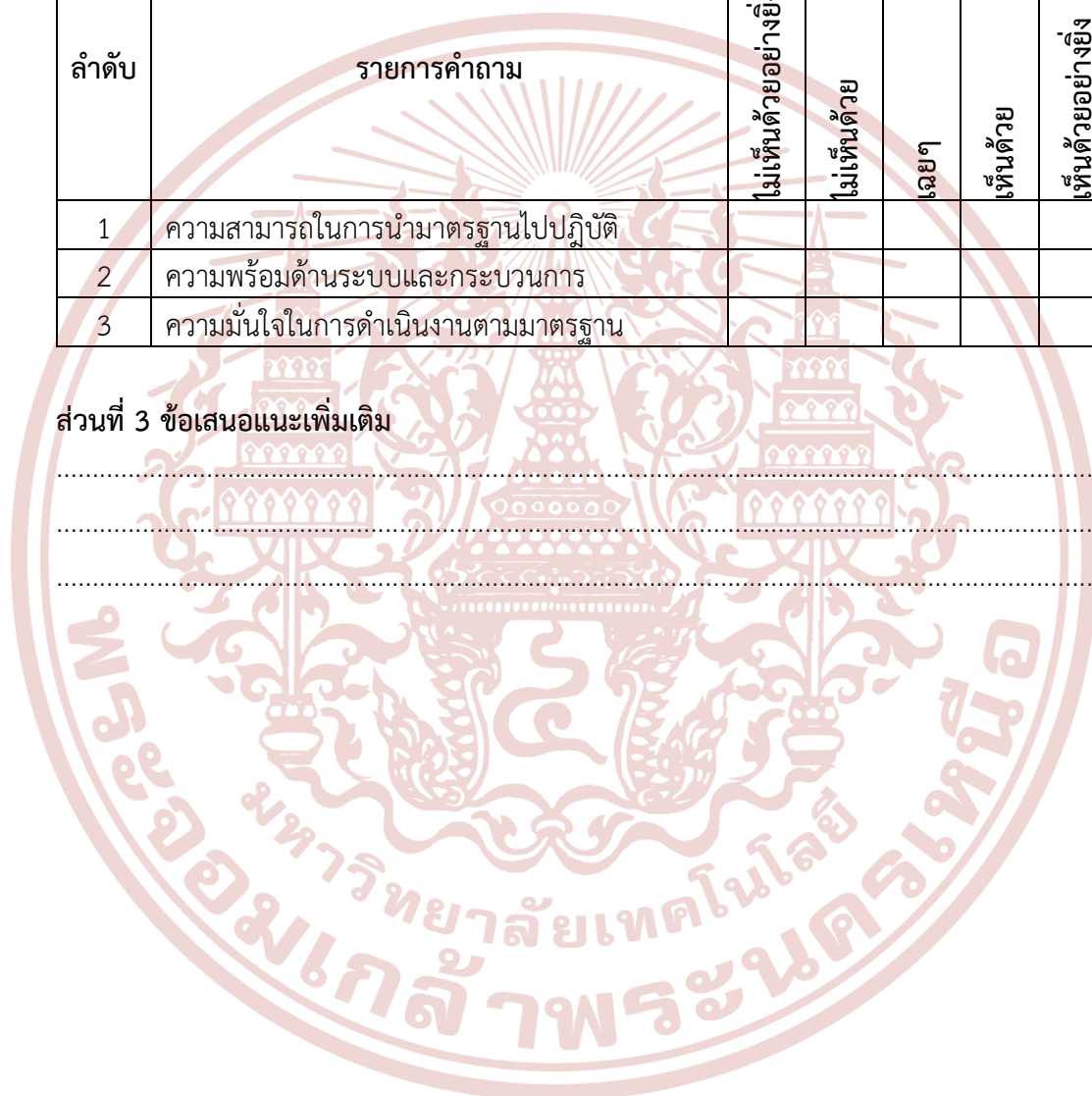
3. ปัจจัยด้านการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ (Perception of Cybersecurity Standards) หมายถึง ระดับความรู้ ความเข้าใจ และการรับทราบของบุคลากรเกี่ยวกับมาตรฐานหรือแนวปฏิบัติด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับบริบทของโรงพยาบาล ซึ่งส่งผลต่อทัศนคติและความตั้งใจในการนำมาตรฐานไปประยุกต์ใช้

ลำดับ	รายการคำถาม	ระดับความคิดเห็นของท่าน				
		ไม่เห็นด้วยอย่างยิ่ง	ไม่เห็นด้วย	เฉยๆ	เห็นด้วย	เห็นด้วยอย่างยิ่ง
1	การรับรู้มาตรฐาน HAIT Plus					
2	การรับรู้มาตรฐาน ISO/IEC 27001					

4. ปัจจัยด้านความพร้อมในการบริหารจัดการตามมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ หมายถึง ความสามารถขององค์กรในการวางแผน ดำเนินการ ควบคุม และปรับปรุงกระบวนการทำงานให้สอดคล้องกับข้อกำหนดของมาตรฐานความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบและต่อเนื่อง

ลำดับ	รายการคำถาม	ระดับความคิดเห็นของท่าน				
		ไม่เห็นด้วยอย่างยิ่ง	ไม่เห็นด้วย	เฉยๆ	เห็นด้วย	เห็นด้วยอย่างยิ่ง
1	ความสามารถในการนำมาตรฐานไปปฏิบัติ					
2	ความพร้อมด้านระบบและกระบวนการ					
3	ความมั่นใจในการดำเนินงานตามมาตรฐาน					

ส่วนที่ 3 ข้อเสนอแนะเพิ่มเติม



ประวัติผู้เขียน

ชื่อ นางสาวผ่องศรี ประสมบุรณ์

ชื่อการค้นคว้าอิสระ การวิเคราะห์ปัจจัยการรับรู้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับโรงพยาบาล

สาขาวิชา ระบบสารสนเทศเพื่อการจัดการ

ประวัติ ประวัติการศึกษา
ระดับปริญญาตรี หลักสูตรศิลปศาสตรบัณฑิต
มหาวิทยาลัย มหาวิทยาลัยราชภัฏจันทรเกษม

