FACTORS AFFECTING CYBERSECURITY AWARENESS TOWARD INFORMATION SYSTEMS IN HOSPITALS: A CASE STUDY OF SIKARIN HOSPITAL

Chanakan SRIRATANABAN[1] and Nontawat WUTTIRONARIT[1*]

1 Faculty of Science and Technology, Graduate School, University of the Thai Chamber of Commerce, Thailand; ohm.wut01@gmail.com (Corresponding Author)

ABSTRACT

This study aimed to: 1) examine cybersecurity awareness regarding hospital information systems; 2) investigate factors influencing cybersecurity awareness; and 3) identify approaches to developing effective factors that promote cybersecurity awareness. The sample consisted of 830 personnel at Sikarin Hospital who used its internal information systems. Data were analyzed using descriptive statistics, including frequency, percentage, mean, and standard deviation, and inferential statistics. The dependent variable's composite score was calculated by averaging the mean scores of its four dimensions. Pearson's correlation coefficient and multiple linear regression were used for hypothesis testing at the .05 significance level. The results showed that respondents reported a low overall level of opinion regarding factors influencing cybersecurity awareness (mean = 2.49). Among individual dimensions, attitudes toward cybersecurity had the highest mean (4.02), while hospital information system usage behavior had the lowest (1.62). Overall cybersecurity awareness was high (mean = 3.89), with tools and technology receiving the highest mean (3.98) and learning and training the lowest (3.80). Of the seven factors examined, four had significant positive relationships with and positive effects on overall cybersecurity awareness: 1) information security knowledge; 2) exposure to cybersecurity-related information; 3) attitudes toward cybersecurity; and 4) positive cybersecurity-related behavior.

Keywords: Awareness, Cybersecurity, Information Systems

CITATION INFORMATION: Sriratanaban, C., & Wuttironarit, N. (2026). Factors Affecting Cybersecurity Awareness toward Information Systems in Hospitals: A Case Study of Sikarin Hospital. *Procedia of Multidisciplinary Research, 4*(10), 30

ปัจจัยที่มีผลต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล กรณีศึกษาโรงพยาบาลศิครินทร์

ชนะกัญจน์ ศรีรัตนบัลล์[1] และ นนทวัตริ์ วุฒิรณฤทธิ์[1*]

1 คณะวิทยาศาตร์และเทคโนโลยี บัณฑิตวิทยาลัย มหาวิทยาลัยหอการค้าไทย; ohm.wut01@gmail.com (ผู้ประพันธ์บรรณกิจ)

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล 2) ศึกษาปัจจัยที่ส่งผลต่อการตระหนักรู้ดังกล่าว และ 3) ศึกษาแนวทางการสร้างปัจจัยที่ส่งเสริมการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ กลุ่มตัวอย่างคือบุคลากรโรงพยาบาลศิครินทร์ที่ใช้งานระบบสารสนเทศภายในโรงพยาบาล จำนวน 830 คน วิเคราะห์ข้อมูลด้วยสถิติเชิงพรรณนา ได้แก่ ความถี่ ร้อยละ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน และสถิติเชิงอนุมาน ได้แก่ สัมประสิทธิ์สหสัมพันธ์เพียร์สันและการถดถอยพหุคูณเชิงเส้น โดยกำหนดระดับนัยสำคัญทางสถิติที่ .05 ทั้งนี้ คะแนนรวมของตัวแปรตามคำนวณจากค่าเฉลี่ยของทั้ง 4 มิติ ผลการศึกษาพบว่า บุคลากรมีความคิดเห็นเกี่ยวกับปัจจัยที่ส่งผลต่อการตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์โดยรวมอยู่ในระดับน้อย (ค่าเฉลี่ย = 2.49) โดยด้านทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์มีค่าเฉลี่ยสูงสุด (4.02) และด้านพฤติกรรมการใช้งานระบบสารสนเทศในโรงพยาบาลมีค่าเฉลี่ยต่ำสุด (1.62) ส่วนลักษณะการตระหนักรู้โดยรวมอยู่ในระดับมาก (ค่าเฉลี่ย = 3.89) โดยด้านเครื่องมือและเทคโนโลยีมีค่าเฉลี่ยสูงสุด (3.98) และด้านการเรียนรู้และการฝึกอบรมมีค่าเฉลี่ยต่ำสุด (3.80) จากปัจจัยทั้ง 7 ด้าน พบว่า 4 ด้านมีความสัมพันธ์และส่งผลทางบวกต่อลักษณะการตระหนักรู้โดยรวม ได้แก่ 1) ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ 2) การรับรู้ข้อมูลข่าวสารด้านความมั่นคงปลอดภัยทางไซเบอร์ 3) ทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และ 4) พฤติกรรมเชิงบวกต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์

คำสำคัญ: การตระหนักรู้, การรักษาความมั่นคงปลอดภัยทางไซเบอร์, ระบบสารสนเทศ

ข้อมูลการอ้างอิง: ชนะกัญจน์ ศรีรัตนบัลล์ และ นนทวัตริ์ วุฒิรณฤทธิ์. (2569). ปัจจัยที่มีผลต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล กรณีศึกษาโรงพยาบาลศิครินทร์. *Procedia of Multidisciplinary Research, 4*(10), 30

บทนำ

เมื่อวันที่ 5 กันยายน พ.ศ.2563 โรงพยาบาลสระบุรีถูก Ransomware VoidCrypt Spade โจมตีทำให้ข้อมูลการรักษาพยาบาลของผู้ป่วย เช่น ประวัติการรักษา รายการยาของผู้ป่วยถูกเข้ารหัส (Encrypt) ผลจากการถูกโจมตีทำให้ไม่สามารถเปิดระบบเชื่อมโยงข้อมูลภายในโรงพยาบาล จากเหตุการณ์ครั้งนี้ทำให้โรงพยาบาลสระบุรีเกิดความสูญเสียด้านการเงินในช่วงเวลาที่ถูกโจมตีทางไซเบอร์เทียบกับช่วงเวลาเดียวกันของปีก่อนเกิดเหตุการณ์ และปีถัดมาหลังเกิดเหตุการณ์ พบว่า สูญเสียรายได้ที่เก็บจากการให้บริการตรวจรักษาผู้ป่วยนอกกับผู้ป่วยเปรียบเทียบจากในช่วงเดือนกันยายนของปี พ.ศ.2562 ถึง ปี พ.ศ.2564 พบว่า ในปี พ.ศ.2562 มีรายได้เป็นจำนวนเงิน 100,609,331 บาท ปี พ.ศ. 2563 รายได้ลดลงเหลือ 32,226,711 บาท และในปี พ.ศ.2564 รายได้ 171,721,044 บาท เห็นได้ชัดว่า ปีที่เกิดการโจมตีรายได้ของโรงพยาบาลลดลงเป็นอย่างมาก ความสำเร็จของการโจมตีทางไซเบอร์ส่วนหนึ่งมีสาเหตุมาจากบุคลากรภายในองค์กร ดังเช่นกรณีที่โรงพยาบาลสระบุรีถูกโจมตีทำให้เกิดภาวะวิกฤตของระบบสารสนเทศนั้น พบว่าสาเหตุหลักมาจากบุคลากรขาดความรู้ ความเข้าใจและขาดความตระหนักเกี่ยวกับความปลอดภัยของระบบสารสนเทศ โดยมีเหตุการณ์ คือ เมื่อมีการพบสิ่งผิดปกติบนคอมพิวเตอร์ที่ใช้งาน แต่ไม่มีการรายงานถึงสิ่งผิดปกติที่เกิดขึ้นนำไปสู่ขั้นตอนการโจมตีเข้าสู่ระบบสารสนเทศของโรงพยาบาล (สมศรี พันธุ์ศักดิ์ศิริ และ เสาวนีย์ สมันต์ตรีพร, 2566) จากการศึกษายังพบว่า ปัญหาที่สำคัญในการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับองค์กร เกิดมาจากบุคลากรภายในองค์กร โดยมีการคาดการณ์ว่าการละเมิดการรักษาความมั่นคงปลอดภัยสารสนเทศเกิดจากบุคลากรไม่ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ ซึ่งการละเมิดนโยบายดังกล่าวเกิดจากความประมาท ความไม่รู้หรือความละเลยของบุคลากร (คณัสนันท์ ทองคำ, 2561) สอดคล้องกับการศึกษาอีกหนึ่งงาน พบว่า ปัจจัยที่ทำให้องค์กรไม่สามารถรักษาความมั่นคงระบบสารสนเทศมาจากบุคลากรในองค์กร โดยสามารถแยกเป็นเรื่องพฤติกรรมการใช้งานระบบสารสนเทศ ความรู้และความตระหนักเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ (นางวิไล ฤทธิเดช, 2565) ผู้วิจัยได้มีโอกาสสัมภาษณ์นายสุริยันต์ โคจรโรจน์ เลขานุการบริษัท บริษัท ศิครินทร์ จำกัด (มหาชน) เมื่อวันที่ 30 ตุลาคม พ.ศ.2566 โรงพยาบาลมีความตระหนักและเข้าใจถึงความเสี่ยงที่จะถูกโจมตีทางไซเบอร์ต่อระบบสารสนเทศของโรงพยาบาล เพื่อป้องกันไม่ให้บุคลากรของตนขาดความตระหนักในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศนายสุริยันต์ฯ จึงประสงค์และยินยอมให้มีการเก็บข้อมูลเพื่อทำการศึกษา ด้วยเหตุการณ์และหลายผลการศึกษาผู้วิจัยจึงมีความสนใจศึกษาปัจจัยที่ส่งผลต่อลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์

วัตถุประสงค์

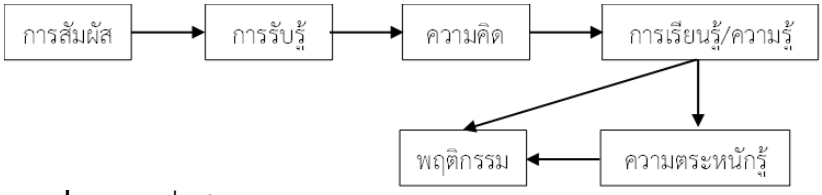
1) เพื่อศึกษาลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล

2) เพื่อศึกษาปัจจัยการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล

3) เพื่อศึกษาแนวทางการสร้างปัจจัยการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ดีที่ส่งผลต่อลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล

การทบทวนวรรณกรรม

แนวคิดเกี่ยวกับความตระหนักรู้ ตามปัจจัยที่ทำให้เกิดความตระหนักรู้ของ Good (1973 อ้างถึงใน ฐิติมา ภู่ห้อย, 2564: 36) อธิบายว่า ความตระหนักรู้เกิดจากกระบวนการทางปัญญา (Cognitive Process) เมื่อบุคคลได้รับสิ่งเร้า จะเกิดการรับรู้ ความเข้าใจ การสร้างความคิดรวบยอด นำไปสู่ความรู้ และท้ายที่สุดเกิดความตระหนักรู้ ซึ่งจะส่งผลต่อพฤติกรรมตามแผนภาพด้านล่าง



ภาพที่ 1 ปัจจัยที่ทำให้เกิดความตระหนักรู้
ที่มา: Good (1973 อ้างถึงใน ฐิติมา ภู่ห้อย, 2564: 36)

แนวคิดแบบจำลองบันได 5 ขั้น (Farrior, 2005 as cited in Khan et al. 2011; Fishbein & Ajzen, 1975) จากทฤษฎีพฤติกรรมตามแผน (Theory of planned behavior หรือ TPB) และโมเดล ความรู้ ทัศนคติและพฤติกรรม (Model of knowledge-attitude behavior หรือ KAB) ถูกนำเสนอในรูปแบบบันไดขั้นตอน 5 ขั้น ซึ่งเป็นโมเดลที่ใช้ประเมินประสิทธิภาพของระดับการตระหนักถึงการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ การเปลี่ยนแปลงพฤติกรรมขึ้นอยู่กับความตั้งใจของแต่ละบุคคล ซึ่งระดับความตั้งใจและพฤติกรรมนั้นสามารถนำมาใช้เป็นตัวชี้วัดระดับการตระหนักถึงการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศได้ (Khan et al., 2011) กล่าวได้ว่า การตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ คือ ความรู้ ความเข้าใจที่ส่งผลต่อทัศนคติเชิงบวกเกี่ยวกับกฎเกณฑ์ ซึ่งจะนำไปสู่ความตั้งใจที่จะปฏิบัติตามและสะท้อนให้เห็นถึงการตระหนักถึงความสำคัญของการปฏิบัติตามกฎเกณฑ์เหล่านั้น โดยการแสดงออกมาในรูปแบบของพฤติกรรมในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ



ภาพที่ 2 Effectiveness of information security awareness methods based on psychological theories.
ที่มา: Khan et al. (2011)

คุณลักษณะเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ จตุชัย แพงจันทร์ (2558 อ้างถึงใน วิไล ฤทธิเดช, 2565: 7) กล่าวไว้ว่า คุณลักษณะของการรักษาความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย 3 อย่าง 1) การรักษาความลับ (Confidentiality) หมายถึง บุคคลที่ไม่ได้รับอนุญาตให้ใช้งานระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ เพื่อป้องกันการเข้าถึงข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์ 2) การรักษาความครบถ้วน (Integrity) หมายถึง เมื่อต้องการใช้งาน ประมวลผล ส่งต่อและการเก็บรักษาข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์ ข้อมูลที่กล่าวมาจะต้องอยู่ในสภาพที่ถูกต้อง ซึ่งข้อมูลดังกล่าวจะถูกต้องได้ต้องอาศัยกระบวนการทำงานเพื่อไม่ให้มีการแก้ไขเปลี่ยนแปลงหรือทำลายข้อมูลจากผู้ที่ไม่ได้รับอนุญาต 3) การรักษาความพร้อมใช้งาน (Availability) หมายถึง กระบวนการที่ทำให้ระบบสารสนเทศรวมไปถึงอุปกรณ์ที่เกี่ยวกับสารสนเทศ สามารถใช้งานได้ทันทีตามเวลาที่ผู้มีสิทธิใช้งานต้องการ

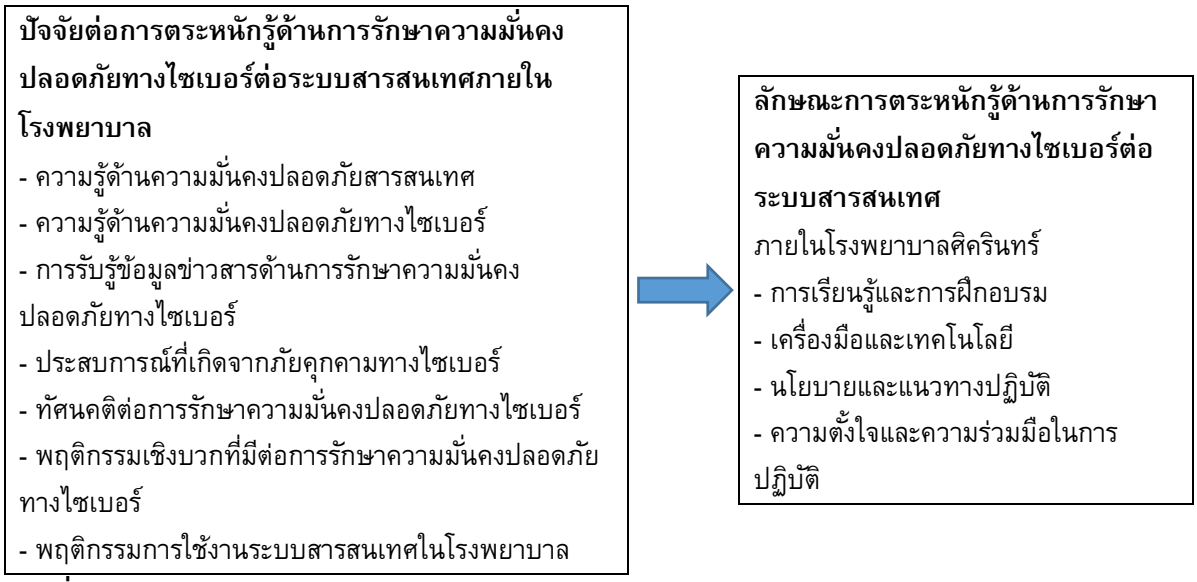
แนวคิดเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ให้ความหมายว่า ภัยคุกคามทางไซเบอร์จากภายในประเทศหรือภายนอกประเทศที่ส่งผลกระทบต่อความมั่นคงของประเทศ ทั้งทางด้านเศรษฐกิจ ทางด้านการทหาร รวมไปถึงความสงบเรียบร้อยในสังคม จะถูกป้องกัน รับมือและลดความเสี่ยงด้วยมาตรการหรือการดำเนินการที่มีการกำหนดขึ้น (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2562: 1-12)

สำนักงานราชบัณฑิตยสภาพจนานุกรมศัพท์คอมพิวเตอร์และเทคโนโลยีสารสนเทศ (2562) ให้ความหมายว่า การที่บุคลากร กระบวนการทำงานและเครื่องมือมีความพร้อมอย่างเหมาะสมในการป้องกันเครือข่าย ระบบคอมพิวเตอร์ โปรแกรม และข้อมูล ไม่ให้ถูกคุกคาม โดยมีลักษณะที่สำคัญ ได้แก่ 1) การคงความลับ 2) การคงความถูกต้อง 3) การคงความพร้อมใช้งานสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union) หรือ ITU ให้ความหมายว่า เครื่องมือต่างๆ นโยบาย แนวคิดเกี่ยวกับการรักษาความปลอดภัย ความมั่นคง การบริหารความเสี่ยง การฝึกอบรมและวิธีปฏิบัติ ในการปกป้องสิ่งแวดล้อมที่เกี่ยวระบบคอมพิวเตอร์และระบบการสื่อสารโทรคมนาคมขององค์กร (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2562: 1-11)

การสร้างลักษณะการตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ จากการศึกษาของ Quick (2020) กล่าวว่า การสร้างลักษณะการตระหนักรู้ด้านความมั่นคงปลอดภัยในการใช้สารสนเทศภายในองค์กร ช่วยให้องค์กรมีความพร้อมและลดโอกาสในการถูกโจมตีทางไซเบอร์ ความตระหนักรู้ของคนในองค์กรมาจากการฝึกอบรมเพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์เป็นการให้ความรู้แก่พนักงานในองค์กร องค์กรยังต้องมีเครื่องมือและเทคโนโลยีในการช่วยให้เกิดความมั่นคงปลอดภัยรวมถึงการมีนโยบายที่ดีเพื่อสนับสนุนการสร้างความตระหนักรู้และการรักษาความมั่นคงปลอดภัยทางไซเบอร์ สุดท้ายคนในองค์กรเมื่อมีความพร้อมด้านความรู้จากการฝึกอบรม เครื่องมือเทคโนโลยี นโยบาย คนในองค์กรจะเกิดความตั้งใจและร่วมมือกันรักษาความมั่นคงปลอดภัยไซเบอร์ แนวคิดดังกล่าวสอดคล้องกับการศึกษาของ ปรมัตถ์ ไวรักษ์ (2562) และ ชรินทร์ทิพย์ ปั้นสุวรรณ (2565) สอดคล้องกันสามารถอธิบายได้ว่า องค์กรอย่างสถาบันการเงินในประเทศไทยหรือองค์กรในยุคดิจิทัลใช้หลักการว่า องค์กรต้องมีการตรวจสอบความพร้อมการรับมือภัยคุกคามอยู่เสมอ จัดการอบรมให้แก่พนักงานในองค์กร ลงทุนด้านเทคโนโลยีการป้องกัน กำหนดนโยบายชัดเจน และเน้นย้ำการทำงานร่วมกันของทุกคนในองค์กร กล่าวได้ว่า ลักษณะการตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์มาจากการฝึกอบรม เทคโนโลยี นโยบาย และความร่วมมือ

ประเภทของการเกิดภัยคุกคามทางไซเบอร์ สุธาเทพ รุณเรศ (2561: 8-9) อธิบายว่า ภัยคุกคามทางไซเบอร์แบ่งออกเป็น 4 กลุ่ม ดังนี้ 1) ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์ มักถูกดาวน์โหลดมาติดตั้งบนคอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่ ซึ่งการติดตั้งอาจมีโปรแกรมที่เป็นภัยคุกคามแอบแฝงมาด้วย โปรแกรมที่เป็นภัยคุกคามนี้เรียกว่ามัลแวร์ เช่น ไวรัส, เวิร์ม, โทรจัน, บอทเน็ต, สปายแวร์ เป็นต้น 2) ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์ เกิดจากผู้ใช้งานคอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่ กดเข้าใช้งานเว็บไซต์ปลอมที่ถูกออกแบบมาให้มีลักษณะคล้ายกับเว็บไซต์จริง เราเรียกว่าเว็บไซต์ปลอมนี้ว่า เว็บฟิชชิ่ง 3) ภัยคุกคามจากการใช้งานเครือข่ายไร้สาย การให้บริการเครือข่ายไร้สายมีจำนวนมาก ผู้ที่ใช้คอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่ ที่มีความต้องการใช้งานเครือข่ายไร้สายจะต้องตรวจสอบให้ดีก่อนจะใช้งาน ถ้าเกิดใช้งานเครือข่ายที่ไม่ปลอดภัยอาจทำให้ผู้ใช้งานเครือข่ายถูกโจมตีด้วยมัลแวร์ จากนั้นผู้ถูกโจมตีสามารถกลายเป็นผู้โจมตีต่อกันไปได้ผ่านเครือข่ายไร้สายที่เชื่อมโยงกัน 4) ภัยคุกคามที่เกิดจากการถูกโจมตีแบบเจาะจงเป้าหมายเป็นภัยคุกคามที่มีความต้องการชัดเจนในการเลือกเป้าหมาย ซึ่งเป้าหมายที่สำคัญที่ถูกเลือกจะเกี่ยวกับโครงสร้างพื้นฐานที่สำคัญ ภัยคุกคามประเภทนี้ถือว่าเป็นภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของประเทศเป็นอย่างยิ่ง

กรอบแนวคิดการวิจัย



ภาพที่ 3 กรอบแนวคิด

สมมติฐานการวิจัย

1) ปัจจัยต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล ด้านความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ มีความสัมพันธ์และส่งผลทางบวกต่อลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์

2) ปัจจัยต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล ด้านความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ มีความสัมพันธ์และส่งผลทางบวกต่อลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์

3) ปัจจัยต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล ด้านการรับรู้ข้อมูลข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีความสัมพันธ์และส่งผลทางบวกต่อลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์

4) ปัจจัยต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล ด้านประสบการณ์ที่เกิดจากภัยคุกคามทางไซเบอร์ มีความสัมพันธ์และส่งผลทางบวกต่อลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์

5) ปัจจัยต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล ด้านทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีความสัมพันธ์และส่งผลทางบวกต่อลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์

6) ปัจจัยต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล ด้านพฤติกรรมเชิงบวกที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีความสัมพันธ์และส่งผลทางบวกต่อลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์

7) ปัจจัยต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล ด้านพฤติกรรมการใช้งานระบบสารสนเทศในโรงพยาบาล มีความสัมพันธ์และส่งผลทางบวกต่อลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงปริมาณ (Quantitative Research) ประชากรที่ใช้ในการศึกษาครั้งนี้คือบุคลากรของโรงพยาบาลศิครินทร์ที่ใช้งานระบบสารสนเทศภายในโรงพยาบาล ในปี 2566 ซึ่งมีจำนวน 1,746 คน (ข้อมูลจากบริษัท ศิครินทร์ จำกัด (มหาชน), 2566) กลุ่มตัวอย่างที่ใช้ในการวิจัยนี้ใช้วิธีการสุ่มตัวอย่างแบบชั้นภูมิ (Stratified sampling) ทำการเลือกตั้งแต่ระดับผู้บริหารจนถึงบุคลากรตามสายงานต่างๆ ของโรงพยาบาลศิครินทร์ คำนวณขนาดกลุ่มตัวอย่างโดยใช้สูตรของทาโร ยามาเน่ (Taro Yamane) ที่ระดับความเชื่อมั่น 95% และระดับความคาดเคลื่อนที่ 5% จากการคำนวณพบว่า ขนาดของกลุ่มตัวอย่างที่ได้รับ คือ 326 คน โดยมีความคาดเคลื่อนไม่เกิน 0.05 ที่ระดับความเชื่อมั่น 95% เพื่อความสมบูรณ์ของข้อมูล ผู้วิจัยสามารถเก็บข้อมูลจากกลุ่มตัวอย่างได้ 830 คน ซึ่งถือว่า ผ่านเกณฑ์ตามเงื่อนไขที่กำหนด คือ ไม่น้อยกว่า 326 คน ดังนั้น ผู้วิจัยจึงเลือกใช้กลุ่มตัวอย่างทั้ง 830 คน โดยใช้แบบสอบถาม (Questionnaire) เป็นเครื่องมือในการเก็บรวบรวมข้อมูล ซึ่งผู้วิจัยนำแบบสอบถามที่สร้างขึ้นเสนออาจารย์ที่ปรึกษาหลักและที่ปรึกษารอง เพื่อพิจารณา ตรวจสอบ และข้อเสนอแนะในการปรับปรุง การวิเคราะห์สถิติเชิงพรรณนา (Descriptive Statistics) ใช้ แจกแจงความถี่ (Frequency) ค่าร้อยละ (Percentage) ค่าเฉลี่ย (Mean) และส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) เพื่อใช้อธิบายข้อมูล และการวิเคราะห์ข้อมูลสถิติเชิงอนุมาน (Inferential Statistics) การวิเคราะห์สถิติสหสัมพันธ์ (Pearson's Correlations Coefficient) และการวิเคราะห์การถดถอยพหุคูณเชิงเส้นตรง (Multiple Linear Regression) โดยมีนัยสำคัญทางสถิติที่ระดับ .05 ซึ่งก่อนนำข้อมูลที่เก็บได้ไปวิเคราะห์สถิติเชิงอนุมาน ผู้วิจัยทำการคำนวณคะแนนรวมของตัวแปรตาม(Composite Score) โดยคำนวณจาก ค่าเฉลี่ย (Mean) ของคะแนนในทุกมิติรวมกัน โดยเริ่มจากการหาค่าเฉลี่ยของข้อคำถามในแต่ละมิติก่อน จากนั้นจึงนำค่าเฉลี่ยของทั้ง 4 มิติมาหาค่าเฉลี่ยรวมอีกครั้งหนึ่งเพื่อให้ได้คะแนนตัวแทนของตัวแปรตาม 1 ตัวแปร สำหรับนำไปทดสอบสมมติฐาน

ผลการวิจัย

ผลการวิเคราะห์ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม พบว่า ผู้ตอบแบบสอบถามส่วนใหญ่เป็นเพศหญิง (ร้อยละ 89.9) มีอายุอยู่ระหว่าง 21-30 ปี (ร้อยละ 60) มีระดับการศึกษาระดับปริญญาตรี (ร้อยละ 59.9) ทำงานในสายงานการพยาบาล (ร้อยละ 73.5) มีรายได้ต่อเดือน 15,001-30,000 บาท (ร้อยละ 61.4) มีระยะเวลาการทำงาน 10 ปีขึ้นไป (ร้อยละ 27.7) และเคยอบรมเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ตามหน่วยงานอื่นจัด (ร้อยละ 58.3)

ผลการวิเคราะห์ข้อมูลเชิงพรรณนาและสถิติเชิงอนุมาน

ตารางที่ 1 ความคิดเห็นเกี่ยวกับปัจจัยต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลโดยรวม

ปัจจัยต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล	$\bar{X}$	S.D.	ระดับ
1) ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ	3.54	0.767	มาก
2) ความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์	1.65	0.839	น้อยที่สุด
3) การรับรู้ข้อมูลข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์	2.34	0.974	น้อย
4) ประสบการณ์ที่เกิดจากภัยคุกคามทางไซเบอร์	1.83	0.747	น้อย
5) ทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์	4.02	0.797	มาก
6) พฤติกรรมเชิงบวกที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์	2.40	0.412	น้อย
7) พฤติกรรมการใช้งานระบบสารสนเทศในโรงพยาบาล	1.62	0.520	น้อยที่สุด
เฉลี่ย	**2.49**	**0.368**	**น้อย**

จากตารางที่ 1 พบว่า บุคลากรของโรงพยาบาลศิครินทร์ที่ตอบแบบสอบถามมีความคิดเห็นด้วยเกี่ยวกับปัจจัยต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล อยู่ในระดับน้อย (ค่าเฉลี่ย = 2.49) เมื่อพิจารณารายด้านสามารถเรียงลำดับจากด้านที่มีค่าเฉลี่ยมากไปหาน้อยที่สุดได้ดังต่อไปนี้ ทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (ค่าเฉลี่ย = 4.02) รองลงมา ได้แก่ ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ (ค่าเฉลี่ย = 3.54), พฤติกรรมเชิงบวกที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (ค่าเฉลี่ย = 2.40), การรับรู้ข้อมูลข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (ค่าเฉลี่ย = 2.34), ประสบการณ์ที่เกิดจากภัยคุกคามทางไซเบอร์ (ค่าเฉลี่ย = 1.83), ความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ (ค่าเฉลี่ย = 1.65) และพฤติกรรมการใช้งานระบบสารสนเทศในโรงพยาบาล (ค่าเฉลี่ย = 1.62) ตามลำดับ

ตารางที่ 2 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานปัจจัยความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ

ปัจจัยความรู้ความมั่นคงปลอดภัยสารสนเทศ	$\bar{X}$	S.D.	ระดับ
1) บุคลากรที่ไม่มีความรู้ด้านความมั่นคงปลอดภัยสารสนเทศเป็นภัยคุกคามความมั่นคงสารสนเทศของโรงพยาบาล	3.01	1.198	ปานกลาง
2) นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยสารสนเทศที่ไม่มีการนำมาใช้อย่างจริงจังเป็นภัยคุกคามความมั่นคงสารสนเทศของโรงพยาบาล	3.35	1.067	ปานกลาง
3) เครื่องมือและเทคโนโลยีที่ล้าสมัยเป็นภัยคุกคามความมั่นคงสารสนเทศของโรงพยาบาล	3.44	1.076	มาก
4) แอพพลิเคชั่นหรือโปรแกรมคอมพิวเตอร์ที่ให้ติดตั้งฟรีโดยไม่รู้ที่มาเป็นภัยคุกคามความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาล	3.84	1.017	มาก
5) ไวรัสคอมพิวเตอร์เป็นภัยคุกคามความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาล	4.11	0.931	มาก
เฉลี่ย	**3.54**	**0.767**	**มาก**

จากตารางที่ 2 พบว่า กลุ่มตัวอย่างมีความคิดเห็นในระดับมาก (ค่าเฉลี่ย = 3.54) เมื่อพิจารณาจากด้านที่มีค่าเฉลี่ยมากที่สุดกับน้อยที่สุดหมายความว่า กลุ่มตัวอย่างมีความคิดเห็นว่าไวรัสคอมพิวเตอร์เป็นภัยคุกคามความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาล มากที่สุด (ค่าเฉลี่ย = 4.11) และบุคลากรที่ไม่มีความรู้ด้านความมั่นคงปลอดภัยสารสนเทศเป็นภัยคุกคามความมั่นคงสารสนเทศของโรงพยาบาล น้อยที่สุด (ค่าเฉลี่ย = 3.01)

ตารางที่ 3 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานปัจจัยความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์

ปัจจัยความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์	$\bar{X}$	S.D.	ระดับ
1) Spyware	1.82	1.005	น้อย
2) Ransomware	1.61	0.990	น้อยที่สุด
3) DDOS	1.52	0.892	น้อยที่สุด
4) Social engineering	1.78	1.005	น้อยที่สุด
5) Phishing	1.53	0.951	น้อยที่สุด
เฉลี่ย	**1.65**	**0.839**	**น้อยที่สุด**

จากตารางที่ 3 พบว่า กลุ่มตัวอย่างมีความคิดเห็นในระดับน้อยที่สุด (ค่าเฉลี่ย = 1.65) เมื่อพิจารณาจากด้านที่มีค่าเฉลี่ยมากที่สุดกับน้อยที่สุดหมายความว่า กลุ่มตัวอย่างมีความเข้าใจเกี่ยวกับ Spyware มากที่สุด (ค่าเฉลี่ย = 1.82) และ DDOS น้อยที่สุด (ค่าเฉลี่ย = 1.52)

ตารางที่ 4 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานปัจจัยการรับรู้ข้อมูลข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ปัจจัยการรับรู้ข้อมูลข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์	$\bar{X}$	S.D.	ระดับ
1) ผู้บริหาร	1.94	1.085	น้อย
2) หัวหน้างาน	2.36	1.214	น้อย
3) เพื่อนร่วมงาน	2.45	1.269	น้อย
4) ป้ายประกาศ (โปสเตอร์)	2.16	1.151	น้อย
5) อินเทอร์เน็ต (เว็บไซต์, เฟสบุ๊ค, ยูทูป, ติ๊กต๊อก)	2.84	1.346	ปานกลาง
เฉลี่ย	**2.34**	**0.974**	**น้อย**

จากตารางที่ 4 พบว่า กลุ่มตัวอย่างมีความคิดเห็นในระดับน้อย (ค่าเฉลี่ย = 2.34) เมื่อพิจารณาจากด้านที่มีค่าเฉลี่ยมากที่สุดกับน้อยที่สุดหมายความว่า กลุ่มตัวอย่างมีการรับรู้จากอินเทอร์เน็ต (เว็บไซต์, เฟสบุ๊ค, ยูทูป, ติ๊กต๊อก) มากที่สุด (ค่าเฉลี่ย = 2.84) และ ผู้บริหาร น้อยที่สุด (ค่าเฉลี่ย = 1.94)

ตารางที่ 5 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานปัจจัยประสบการณ์ที่เกิดจากภัยคุกคามทางไซเบอร์

ปัจจัยประสบการณ์ที่เกิดจากภัยคุกคามทางไซเบอร์	$\bar{X}$	S.D.	ระดับ
1) ได้รับผลกระทบจากไวรัสทำให้ไฟล์งานหรือข้อมูลการทำงานใช้งานไม่ได้รวมไปถึงข้อมูลสูญหาย	1.61	0.815	น้อยที่สุด
2) โดนขโมยข้อมูลส่วนตัว เช่น บัญชีผู้ใช้งาน รหัสผ่าน หมายเลขโทรศัพท์ หรือข้อมูลทางการเงิน	1.52	0.867	น้อยที่สุด
3) ได้รับจดหมายอิเล็กทรอนิกส์ (E-mail) หลอกลวง	2.04	1.159	น้อย
4) ได้รับโฆษณาที่ไม่พึงประสงค์ผ่านทางจดหมายอิเล็กทรอนิกส์ (E-mail) หรือแอพพลิเคชั่นออนไลน์ เช่น Facebook	2.38	1.217	น้อย
5) ถูกหลอกให้เข้าเว็บไซต์ปลอมเพื่อกรอกข้อมูลส่วนตัว	1.63	0.928	น้อยที่สุด
เฉลี่ย	**1.83**	**0.747**	**น้อย**

จากตารางที่ 5 พบว่า กลุ่มตัวอย่างมีความคิดเห็นในระดับน้อย (ค่าเฉลี่ย = 1.83) เมื่อพิจารณาจากด้านที่มีค่าเฉลี่ยมากที่สุดกับน้อยที่สุดหมายความว่า กลุ่มตัวอย่างมีประสบการณ์การได้รับโฆษณาที่ไม่พึงประสงค์ผ่านทางจดหมายอิเล็กทรอนิกส์ (E-mail) หรือ แอพพลิเคชั่นออนไลน์ เช่น Facebook มากที่สุด (ค่าเฉลี่ย = 2.38) และ โดนขโมยข้อมูลส่วนตัว เช่น บัญชีผู้ใช้งาน รหัสผ่าน หมายเลขโทรศัพท์ หรือข้อมูลทางการเงิน น้อยที่สุด (ค่าเฉลี่ย = 1.52)

ตารางที่ 6 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานปัจจัยทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ปัจจัยทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์	$\bar{X}$	S.D.	ระดับ
1) การรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลเป็นหน้าที่ของบุคลากรทุกคน	3.92	1.020	มาก
2) ท่านยินดีปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างเคร่งครัด	4.05	0.914	มาก
3) การรักษาความมั่นคงปลอดภัยทางไซเบอร์จะเป็นประโยชน์ต่อโรงพยาบาลและตัวท่านเอง	4.17	0.861	มาก
4) บุคลากรทุกคนจำเป็นต้องได้รับการอบรมเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศอย่างสม่ำเสมอ	3.97	0.900	มาก
5) การรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นเรื่องที่น่าเรียนรู้และทำความเข้าใจ	4.00	0.885	มาก
เฉลี่ย	**4.02**	**0.797**	**มาก**

จากตารางที่ 6 พบว่า กลุ่มตัวอย่างมีความคิดเห็นในระดับมาก (ค่าเฉลี่ย = 4.02) เมื่อพิจารณาจากด้านที่มีค่าเฉลี่ยมากที่สุดกับน้อยที่สุดหมายความว่า กลุ่มตัวอย่างคิดเห็นว่าการรักษาความมั่นคงปลอดภัยทางไซเบอร์จะเป็นประโยชน์ต่อโรงพยาบาลและตัวท่านเอง มากที่สุด (ค่าเฉลี่ย = 4.17) และการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลเป็นหน้าที่ของบุคลากรทุกคน น้อยที่สุด (ค่าเฉลี่ย = 3.92)

ตารางที่ 7 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานปัจจัยพฤติกรรมเชิงบวกที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ปัจจัยพฤติกรรมเชิงบวกที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์	$\bar{X}$	S.D.	ระดับ
1. ปิดการใช้งาน (Log out) ทุกครั้ง เมื่อไม่ได้ใช้งานคอมพิวเตอร์ที่อยู่ในระบบสารสนเทศ	2.66	0.517	ปานกลาง
2. ใช้งานการพักหน้าจอ (Lockscreen) กับคอมพิวเตอร์ที่อยู่ในระบบสารสนเทศทุกครั้ง เมื่อไม่ได้อยู่ประจำคอมพิวเตอร์	2.32	0.597	น้อย
3. ตรวจสอบแหล่งที่มาของอีเมล์ URLของลิงก์ในอีเมล์ ที่อยู่เว็บไซต์ ก่อนกดเข้าใช้งาน	2.24	0.694	น้อย
4. ส่งข้อมูลสำคัญที่เกี่ยวกับการทำงานผ่านทางอีเมล์เท่านั้น	2.21	0.646	น้อย
5. แจ้งหน่วยงานด้านเทคโนโลยีสารสนเทศ (IT) ทันที เมื่อพบความผิดปกติบนคอมพิวเตอร์ที่อยู่ในระบบสารสนเทศที่ใช้งานอยู่	2.61	0.600	ปานกลาง
เฉลี่ย	**2.40**	**0.412**	**น้อย**

จากตารางที่ 7 พบว่า กลุ่มตัวอย่างมีความคิดเห็นในระดับมาก (ค่าเฉลี่ย = 2.40) เมื่อพิจารณาจากด้านที่มีค่าเฉลี่ยมากที่สุดกับน้อยที่สุดหมายความว่า กลุ่มตัวอย่างมีพฤติกรรมเชิงบวกคือปิดการใช้งาน (Log out) ทุกครั้ง เมื่อไม่ได้ใช้งานคอมพิวเตอร์ที่อยู่ในระบบสารสนเทศ มากที่สุด (ค่าเฉลี่ย = 2.66) และส่งข้อมูลสำคัญที่เกี่ยวกับการทำงานผ่านทางอีเมล์เท่านั้น น้อยที่สุด (ค่าเฉลี่ย = 2.21)

ตารางที่ 8 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานปัจจัยพฤติกรรมการใช้งานระบบสารสนเทศในโรงพยาบาล

ปัจจัยพฤติกรรมการใช้งานระบบสารสนเทศในโรงพยาบาล	$\bar{X}$	S.D.	ระดับ
1) ตั้งรหัสผ่านโดยใช้ตัวอักษรหรือตัวเลขที่เกี่ยวข้องกับข้อมูลส่วนตัว เช่น ตั้งตามชื่อ วันเดือนปีเกิด หมายเลขโทรศัพท์ ทะเบียนรถ	2.24	0.724	น้อย
2) จดชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ไว้ตามจุดที่ผู้อื่นอาจเห็นได้ เช่น โต๊ะทำงาน หน้าจอคอมพิวเตอร์ บนปฏิทิน	1.50	0.701	น้อยที่สุด
3) ให้บัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) กับบุคคลอื่น เพื่อเข้าใช้งานระบบสารสนเทศ	1.56	0.693	น้อยที่สุด
4) โหลดแอพพลิเคชั่นหรือโปรแกรมคอมพิวเตอร์โดยไม่ผ่านหน่วยงานด้านเทคโนโลยีสารสนเทศ (IT)	1.44	0.666	น้อยที่สุด
5) กดลิงค์โฆษณาขณะใช้งาน Internet Browser	1.40	0.640	น้อยที่สุด
เฉลี่ย	**1.62**	**0.520**	**น้อยที่สุด**

จากตารางที่ 8 พบว่า กลุ่มตัวอย่างมีความคิดเห็นในระดับมาก (ค่าเฉลี่ย = 2.40) เมื่อพิจารณาจากด้านที่มีค่าเฉลี่ยมากที่สุดกับน้อยที่สุดหมายความว่า กลุ่มตัวอย่างมีพฤติกรรมการใช้งานคือตั้งรหัสผ่านโดยใช้ตัวอักษรหรือตัวเลขที่เกี่ยวข้องกับข้อมูลส่วนตัว เช่นตั้งตามชื่อ วันเดือนปีเกิด หมายเลขโทรศัพท์ ทะเบียนรถ มากที่สุด (ค่าเฉลี่ย = 2.24) และกดลิงค์โฆษณาขณะใช้งาน Internet Browser น้อยที่สุด (ค่าเฉลี่ย = 1.40)

ตารางที่ 9 ความคิดเห็นเกี่ยวกับลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์โดยรวม

ลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์	$\bar{X}$	S.D.	ระดับ
1) การเรียนรู้และการฝึกอบรม	3.80	0.807	มาก
2) เครื่องมือและเทคโนโลยี	3.98	0.784	มาก
3) นโยบายและแนวทางปฏิบัติ	3.87	0.769	มาก
4) ความตั้งใจและความร่วมมือในการปฏิบัติ	3.89	0.754	มาก
เฉลี่ย	**3.89**	**0.698**	**มาก**

จากตารางที่ 9 พบว่า บุคลากรของโรงพยาบาลศิครินทร์ที่ตอบแบบสอบถามมีความคิดเห็นด้วยเกี่ยวกับลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์ อยู่ในระดับมาก (ค่าเฉลี่ย = 3.89) เมื่อพิจารณารายด้านสามารถเรียงลำดับจากด้านที่มีค่าเฉลี่ยมากไปหาน้อยที่สุดได้ดังต่อไปนี้ เครื่องมือและเทคโนโลยี (ค่าเฉลี่ย = 3.98) รองลงมา ได้แก่ ความตั้งใจและความร่วมมือในการปฏิบัติ (ค่าเฉลี่ย = 3.89) นโยบายและแนวทางปฏิบัติ (ค่าเฉลี่ย = 3.87) และการเรียนรู้และการฝึกอบรม (ค่าเฉลี่ย = 3.80) ตามลำดับ

ตารางที่ 10 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานด้านการเรียนรู้และการฝึกอบรม

ด้านการเรียนรู้และการฝึกอบรม	$\bar{X}$	**S.D.**	**ระดับ**
1) การฝึกอบรมเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับบุคลากรทุกระดับ	3.86	0.906	มาก
2) หลังการอบรม บุคลากรตระหนักถึงการรักษาความมั่นคงปลอดภัยทางไซเบอร์	3.90	0.879	มาก
3) บุคลากรทุกระดับแบ่งเวลาศึกษาเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ด้วยตนเอง	3.66	0.879	มาก
เฉลี่ย	**3.80**	**0.807**	**มาก**

จากตารางที่ 10 พบว่า กลุ่มตัวอย่างมีความคิดเห็นในระดับมาก (ค่าเฉลี่ย = 3.80) เมื่อพิจารณาจากด้านที่มีค่าเฉลี่ยมากที่สุดกับน้อยที่สุดหมายความว่า กลุ่มตัวอย่างคิดเห็นว่าหลังการอบรม บุคลากรตระหนักถึงการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มากที่สุด (ค่าเฉลี่ย = 3.90) และบุคลากรทุกระดับแบ่งเวลาศึกษาเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ด้วยตนเอง น้อยที่สุด (ค่าเฉลี่ย = 3.66)

ตารางที่ 11 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานด้านเครื่องมือและเทคโนโลยี

ด้านเครื่องมือและเทคโนโลยี	$\bar{X}$	**S.D.**	**ระดับ**
1) เครื่องมือและเทคโนโลยีที่มีความทันสมัย	3.90	0.888	มาก
2) เครื่องมือและเทคโนโลยีที่ใช้ถูกต้องตามลิขสิทธิ์	4.01	0.828	มาก
3) เครื่องมือและเทคโนโลยีที่ใช้มีการอัพเดตอยู่สม่ำเสมอ	3.97	0.890	มาก
4) เครื่องมือและเทคโนโลยีต้องสามารถใช้งานได้ตลอดเวลา	4.07	0.877	มาก
เฉลี่ย	**3.98**	**0.784**	**มาก**

จากตารางที่ 11 พบว่า กลุ่มตัวอย่างมีความคิดเห็นในระดับมาก (ค่าเฉลี่ย = 3.98) เมื่อพิจารณาจากด้านที่มีค่าเฉลี่ยมากที่สุดกับน้อยที่สุดหมายความว่า กลุ่มตัวอย่างคิดเห็นว่าเครื่องมือและเทคโนโลยีต้องสามารถใช้งานได้ตลอดเวลามีผลต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล มากที่สุด (ค่าเฉลี่ย = 4.07) และเครื่องมือและเทคโนโลยีที่มีความทันสมัยมีผลต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล น้อยที่สุด (ค่าเฉลี่ย = 3.66)

ตารางที่ 12 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานด้านนโยบายและแนวทางปฏิบัติ

ด้านนโยบายและแนวทางปฏิบัติ	$\bar{X}$	**S.D.**	**ระดับ**
1) การที่โรงพยาบาลมีนโยบายและแนวทางปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างเป็นลายลักษณ์อักษร	3.85	0.856	มาก
2) บุคลากรทุกระดับเข้าใจนโยบายและแนวทางปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์	3.84	0.840	มาก
3) บุคลากรทุกระดับปฏิบัติตามนโยบายและแนวทางปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างเคร่งครัด	3.89	0.824	มาก
4) นโยบายและแนวทางปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ปรับเปลี่ยนให้เหมาะสมกับบริบทอยู่เสมอ ทำให้เกิดการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ดีขึ้น	3.92	0.825	มาก
เฉลี่ย	**3.87**	**0.769**	**มาก**

จากตารางที่ 12 พบว่า กลุ่มตัวอย่างมีความคิดเห็นในระดับมาก (ค่าเฉลี่ย = 3.87) เมื่อพิจารณาจากด้านที่มีค่าเฉลี่ยมากที่สุดกับน้อยที่สุดหมายความว่า กลุ่มตัวอย่างคิดเห็นว่านโยบายและแนวทางปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ปรับเปลี่ยนให้เหมาะสมกับบริบทอยู่เสมอทำให้เกิดการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ดีขึ้น มากที่สุด (ค่าเฉลี่ย = 3.92) และบุคลากรทุกระดับเข้าใจนโยบายและแนวทางปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ น้อยที่สุด (ค่าเฉลี่ย = 3.84)

ตารางที่ 13 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานด้านความตั้งใจและความร่วมมือ

ด้านความตั้งใจและความร่วมมือ	$\bar{X}$	**S.D.**	**ระดับ**
1) ผู้บริหารให้ความสำคัญเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์มาในระดับนโยบาย	3.89	0.839	มาก
2) บุคลากรด้านเทคโนโลยีสารสนเทศมีความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์มากกว่าบุคลากรสายงานอื่น ทำให้เกิดการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ดีขึ้น	3.89	0.817	มาก
3) บุคลากรทุกคนมีความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ทำให้เกิดการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ดีขึ้น	3.87	0.825	มาก
4) บุคลากรทุกคนตั้งใจและร่วมมือในการปฏิบัติ เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ทำให้เกิดการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ดีขึ้น	3.92	0.839	มาก
เฉลี่ย	**3.89**	**0.754**	**มาก**

จากตารางที่ 13 พบว่า กลุ่มตัวอย่างมีความคิดเห็นในระดับมาก (ค่าเฉลี่ย = 3.89) เมื่อพิจารณาจากด้านที่มีค่าเฉลี่ยมากที่สุดกับน้อยที่สุดหมายความว่า กลุ่มตัวอย่างคิดเห็นว่าบุคลากรทุกคนตั้งใจและร่วมมือในการปฏิบัติ เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ทำให้เกิดการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ดีขึ้น มากที่สุด (ค่าเฉลี่ย = 3.92) และบุคลากรทุกคนมีความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ทำให้เกิดการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ดีขึ้น น้อยที่สุด (ค่าเฉลี่ย = 3.87)

ผลการวิเคราะห์สัมประสิทธิ์ของความเชื่อมั่น (Coefficient of Reliability) นำข้อมูลที่รวบรวมได้จากผู้ตอบแบบสอบถาม จำนวน 830 คน มาทดสอบความน่าเชื่อถือ (Reliability) ตามวิธีของครอนบาช (Cronbach) ในการคำนวณหาค่าสัมประสิทธิ์ของความน่าเชื่อถือ (Cronbach's Alpha Coefficient, α) เพื่อวัดความสอดคล้องภายในของข้อคำถามต่าง ๆ ที่เป็นองค์ประกอบของแต่ละตัวแปรว่ามีความสอดคล้องกันมากน้อยเพียงใด เพื่อใช้ประกอบการตัดสินใจว่าควรจะคงคำถามนั้นเอาไว้หรือตัดออก (ศิริชัย กาญจนวสี, 2554) ผลจากการทดสอบความน่าเชื่อถือได้ค่าสัมประสิทธิ์ของความน่าเชื่อถือ ดังตารางที่ 14

ตารางที่ 14 การวิเคราะห์สัมประสิทธิ์ของความเชื่อมั่น (Coefficient of Reliability)

ปัจจัยที่ศึกษา	**Cronbach's Alpha Coefficient จากการศึกษาจริง**
ตัวแปรอิสระ	
ปัจจัยต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล	
1) ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ	0.772
2) ความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์	0.917

ปัจจัยที่ศึกษา	Cronbach's Alpha Coefficient จากการศึกษาจริง
3) การรับรู้ข้อมูลข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์	0.860
4) ประสบการณ์ที่เกิดจากภัยคุกคามทางไซเบอร์	0.793
5) ทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์	0.919
6) พฤติกรรมเชิงบวกที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์	0.697
7) พฤติกรรมการใช้งานระบบสารสนเทศในโรงพยาบาล	0.816
ตัวแปรตาม 1 ตัว (4 ด้าน) ลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์	
1) การเรียนรู้และการฝึกอบรม	0.895
2) เครื่องมือและเทคโนโลยี	0.922
3) นโยบายและแนวทางปฏิบัติ	0.940
4) ความตั้งใจและความร่วมมือในการปฏิบัติ	0.930

จากตารางที่ 14 พบว่าตัวแปรอิสระ 7 ด้าน มีค่ามากกว่า 0.70 ทั้งหมด 6 ปัจจัย โดยมีปัจจัยที่มีค่าน้อยกว่า 0.70 จำนวน 1 ปัจจัย คือ ปัจจัยพฤติกรรมเชิงบวกที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีค่าเท่ากับ 0.697 ซึ่งผู้วิจัยไม่ได้ตัดปัจจัยดังกล่าวออกเนื่องจากค่าดังกล่าวอยู่ในช่วง 0.60-0.69 ถือว่าอยู่ในเกณฑ์พอรับได้ (George & Mallery, 2003) ในส่วนตัวแปรตามลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์ที่มี 4 ด้าน มีค่ามากกว่า 0.7 จึงนำมาพิจารณาทั้งหมด

ผลการวิเคราะห์สถิติสหสัมพันธ์ (Pearson's Correlations Coefficient)

ตารางที่ 15 การวิเคราะห์สถิติสหสัมพันธ์ (Pearson's Correlations Coefficient)

ปัจจัยที่มีผลต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์	ลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์		
	ค่าความสัมพันธ์ (r)	ค่า Sig.	ระดับความสัมพันธ์
ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ	.430**	<.001	สัมพันธ์ปานกลาง
ความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์	.019	.585	ไม่มีความสัมพันธ์
การรับรู้ข้อมูลข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์	.124**	<.001	สัมพันธ์ต่ำ
ประสบการณ์ที่เกิดจากภัยคุกคามทางไซเบอร์	-.026	.461	ไม่มีความสัมพันธ์
ทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์	.735**	<.001	สัมพันธ์ปานกลาง
พฤติกรรมเชิงบวกที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์	.330**	<.001	สัมพันธ์ปานกลาง
พฤติกรรมการใช้งานระบบสารสนเทศในโรงพยาบาล	-.119**	<.001	สัมพันธ์ต่ำ

จากตารางที่ 15 พบว่า ปัจจัยความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ ปัจจัยการรับรู้ข้อมูลข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ปัจจัยทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พฤติกรรมเชิงบวกที่มี

ต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และปัจจัยด้านพฤติกรรมการใช้งานระบบสารสนเทศในโรงพยาบาล มีค่า Sig. เท่ากับ <.001 ซึ่งน้อยกว่า .05 หมายความว่า ทั้ง 5 ปัจจัย มีความสัมพันธ์กับลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์ อย่างมีนัยสำคัญที่ 0.01 ส่วนปัจจัยด้านความรู้ความมั่นคงปลอดภัยทางไซเบอร์และปัจจัยด้านประสบการณ์ที่เกิดจากภัยคุกคามทางไซเบอร์ มีค่า Sig. เท่ากับ 0.585 และ 0.461 ซึ่งมากกว่า .05 หมายความว่า ทั้ง 2 ปัจจัยไม่มีความสัมพันธ์กับลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์ อย่างมีนัยยะสำคัญที่ระดับ 0.05

ผลการวิเคราะห์การถดถอยพหุคูณเชิงเส้นตรง (Multiple Linear Regression) ผู้วิจัยทราบผลจากการหาความสัมพันธ์ระหว่างปัจจัยที่มีผลต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (ตัวแปรอิสระ) กับลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์ (ตัวแปรตาม) ได้ผลว่าตัวแปรอิสระ 7 ปัจจัย คงเหลือ 5 ปัจจัย (ตามตารางที่ 15) ผู้วิจัยจึงนำปัจจัยอิสระที่เหลือ 5 ปัจจัยหาค่าถดถอยพหุคูณเชิงเส้นตรง (Multiple Linear Regression) เพื่อทดสอบสมมติฐานต่อไป

ตารางที่ 16 ตารางวิเคราะห์ความแปรปรวน (ANOVA) ของ Multiple Linear Regression

Model	Sum of Square	DF	Mean Square	F	Sig.
Regression	232.882	5	46.576	223.602	<.001[b]
Residual	171.640	824	.208		
Total	404.521	829			

จากตารางที่ 16 พบว่า ค่าความแปรปรวนของของการวิเคราะห์การถดถอยเชิงพหุคูณยืนยันว่าตัวแปรอิสระ 5 ตัว ประกอบด้วย ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ การรับรู้ข้อมูลข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พฤติกรรมเชิงบวกที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และพฤติกรรมการใช้งานระบบสารสนเทศในโรงพยาบาล มีอิทธิพลต่อตัวแปรตาม เนื่องจากค่า Sig. ของสมการมีค่าเท่ากับ <.001 อย่างมีนัยสำคัญที่ .01

ตารางที่ 17 การตรวจสอบค่า Tolerance และหาค่า VIF

ตัวแปรอิสระ	Collinearity Statistics	
	Tolerance	VIF
ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ	.794	1.260
การรับรู้ข้อมูลข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์	.937	1.068
ทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์	.726	1.377
พฤติกรรมเชิงบวกที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์	.900	1.112
พฤติกรรมการใช้งานระบบสารสนเทศในโรงพยาบาล	.893	1.120

จากตารางที่ 17 พบว่า ตัวแปรอิสระทั้ง 5 ตัวแปร ได้แก่ ปัจจัยความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ ปัจจัยการรับรู้ข้อมูลข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ปัจจัยทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พฤติกรรมเชิงบวกที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และพฤติกรรมการใช้งานระบบสารสนเทศในโรงพยาบาล มีค่า Tolerance .726-.937 ซึ่งมากกว่าเกณฑ์ขั้นต่ำที่ต้องการที่ 0.1 และ ค่า VIF 1.068-

1.377 ซึ่งน้อยกว่า 10 ตามเกณฑ์ สรุปได้ว่าตัวแปรอิสระทั้ง 5 ตัวแปร ไม่มีความสัมพันธ์กัน และมีความเหมาะสมที่จะนำไปวิเคราะห์เพื่อทดสอบสมมติฐานการวิจัยต่อไป

ตารางที่ 18 ปัจจัยที่มีประสิทธิภาพในการพยากรณ์ลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.759[a]	.576	.573	.45640

a. Predictors: (Constant), ปัจจัยความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ ปัจจัยการรับรู้ข้อมูลข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ปัจจัยทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พฤติกรรมเชิงบวกที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พฤติกรรมการใช้งานระบบสารสนเทศในโรงพยาบาล

จากตารางที่ 18 พบว่า ปัจจัยที่มีประสิทธิภาพในการพยากรณ์ลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์ ทั้ง 5 ปัจจัย คือ ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ, การรับรู้ข้อมูลข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์, ทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์, พฤติกรรมเชิงบวกที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และพฤติกรรมการใช้งานระบบสารสนเทศในโรงพยาบาล ซึ่งมีความสัมพันธ์กับลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์ โดยตัวแปรอิสระทั้ง 5 ปัจจัย สามารถอธิบายการผันแปรของลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์ได้ร้อยละ 57.6 (R2 = 0.576)

ตารางที่ 19 ผลการวิเคราะห์ตัวแปรอิสระที่ส่งผลต่อตัวแปรตาม (Dependent Variable) ลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์

Model	Unstandardized Coefficients		standardized Coefficients	T	Sig.
	B	Std. Error	Beta		
(Constant)	.568	.132		4.306	<.001
ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ	.109	.023	**.119**	4.691	**<.001**
การรับรู้ข้อมูลข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์	.043	.017	**.061**	2.583	**.010**
ทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์	.564	.023	**.644**	24.193	**<.001**
พฤติกรรมเชิงบวกที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์	.228	.040	**.135**	5.631	**<.001**
พฤติกรรมการใช้งานระบบสารสนเทศในโรงพยาบาล	.011	.032	.008	0.349	.727

จากตารางที่ 19 แสดงผลการวิเคราะห์ปัจจัยที่มีประสิทธิภาพในการพยากรณ์ลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์ ด้วยสมมติฐานทางสถิติ พบว่า ปัจจัยที่มีผลต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ที่ส่งผลต่อลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์ก็ต่อเมื่อค่า Sig. มีค่าน้อยกว่า 0.05 จากการทดสอบสมมติฐานพบว่า ปัจจัยความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ มีค่า Sig. = <.001 และมีค่า

คะแนนดิบ (β) = .119, ปัจจัยการรับรู้ข้อมูลข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีค่า Sig. = 0.01 และมีค่าคะแนนดิบ (β) = .061, ปัจจัยด้านทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีค่า Sig. = <.001 และมีค่าคะแนนดิบ (β) = .644 และปัจจัยด้านพฤติกรรมเชิงบวกที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีค่า Sig. = <.001 และมีค่าคะแนนดิบ (β) = .135 ทำให้ทั้ง 4 ปัจจัย ส่งผลต่อลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์ อย่างมีนัยสำคัญทางสถิติที่ 0.05 ทั้งนี้ ปัจจัยพฤติกรรมการใช้งานระบบสารสนเทศในโรงพยาบาล มีค่า Sig. = .727 และมีค่าคะแนนดิบ (β) = .008 ทำให้ปัจจัยดังกล่าวไม่ส่งผลต่อลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์ สำหรับปัจจัยพฤติกรรมการใช้งานระบบสารสนเทศในโรงพยาบาล

สรุปและอภิปรายผลการวิจัย

จากการศึกษา ปัจจัยที่มีผลต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล กรณีศึกษาโรงพยาบาลศิครินทร์ พบว่าตัวแปร 4 ตัว ได้แก่ ปัจจัยความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ, ปัจจัยการรับรู้ข้อมูลข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์, ปัจจัยทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และปัจจัยพฤติกรรมเชิงบวกที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ส่งผลต่อลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์ ดังภาพด้านล่าง

ปัจจัยต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล

- ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ
- การรับรู้ข้อมูลข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์
- ทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์
- พฤติกรรมเชิงบวกที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์



ลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศ

ภายในโรงพยาบาลศิครินทร์

- การเรียนรู้และการฝึกอบรม
- เครื่องมือและเทคโนโลยี
- นโยบายและแนวทางปฏิบัติ
- ความตั้งใจและความร่วมมือในการปฏิบัติ

อภิปรายผลการวิจัย

1) ปัจจัยความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ

จากการศึกษาพบว่า ปัจจัยความรู้ด้านความมั่นคงปลอดภัยสารสนเทศภาพรวมความคิดเห็นอยู่ในระดับมาก ตีความได้ว่าบุคลากรในโรงพยาบาลศิครินทร์เห็นว่าความรู้ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศมีความสำคัญต่อลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์ ก่อนจะตระหนักรู้ได้ต้องมีความรู้ความเข้าใจเพื่อให้เกิดความคิดความตระหนัก จากการศึกษาเป็นไปได้ว่า พนักงานในโรงพยาบาลมีข้อจำกัดในเรื่องความรู้เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ด้วยลักษณะของการทำงานที่ทำงานเกี่ยวกับระบบสาธารณสุขเป็นส่วนใหญ่ แต่ทุกคนกลับเข้าใจเหมือนกันว่าความรู้ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ คือ การรักษาความปลอดภัยของข้อมูลสารสนเทศในโรงพยาบาลจากภัยคุกคามทุกรูปแบบผลการศึกษาเป็นไปตามแนวคิดของ Good (1973) เนื่องจากความรู้เป็นหนึ่งในขั้นตอนที่ทำให้เกิดความตระหนักรู้ รวมถึงยังพบว่าปัจจัยความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ สอดคล้องกับงานวิจัยของ สุธาเทพ รุณเรศ (2561) ซึ่งพบว่า ปัจจัยทางด้านความรู้มีความสัมพันธ์กับปัจจัยทางด้านความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศ

2) ปัจจัยการรับรู้ข้อมูลข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

จากการศึกษาพบว่าปัจจัยการรับรู้ข้อมูลข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ภาพรวมความคิดเห็นอยู่ในระดับน้อย โดยส่วนใหญ่รับรู้ข้อมูลจากอินเทอร์เน็ต (เว็บไซต์, เฟสบุ๊ค, ยูทูป, ติ๊กต๊อก) ตีความได้ว่าบุคลากรในโรงพยาบาลศิครินทร์รับรู้ข่าวสารด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ด้วยตนเองมากกว่าจะรับรู้ด้วยวิธีการอื่นหรือรับรู้จากองค์กร เนื่องจากโรงพยาบาลมีการติดป้ายประชาสัมพันธ์ โปสเตอร์เน้นเรื่องการรักษาพยาบาลเป็นส่วนใหญ่ทำให้พนักงานของโรงพยาบาลต้องหาช่องทางการรับรู้ด้วยวิธีอื่นๆ ปัจจัยด้านการรับรู้ยังเป็นส่วนหนึ่งในขั้นตอนการเกิดการตระหนักรู้ตามแนวคิดของ Good (1973) สอดคล้องกับงานวิจัยของ Bélanger et al. (2022) ที่พบว่า การเปิดรับข่าวสารซ้ำๆ มีความสัมพันธ์เชิงบวกกับความรู้ด้านการปกป้องข้อมูล (contextual knowledge) และความรู้ที่เพิ่มขึ้นมีผลต่อพฤติกรรมการปกป้องข้อมูลในเวลาต่อมา อีกผลการศึกษาของ Bauer Stefan (2016) พบว่า ช่องทางการสื่อสารข้อมูลภายในองค์กร เช่น e-learning, Intranet messages, Security campaigns, หนังสือพิมพ์/วารสารภายใน, Posters มีบทบาทในการสร้างการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมถึงผลการศึกษาของ Julie Haney (2019) พบว่า สื่อและกิจกรรมที่องค์กรเผยแพร่ให้กับบุคลากรในองค์กรเป็นองค์ประกอบในการสร้างความตระหนักรู้ในการรักษาความมั่นคงปลอดภัยสารสนเทศ

3) ปัจจัยทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์

จากการศึกษาพบว่าปัจจัยทัศนคติต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ภาพรวมความคิดเห็นอยู่ในระดับมาก ตีความหมายได้ว่า บุคลากรของโรงพยาบาลศิครินทร์ส่วนใหญ่เข้าใจความสำคัญของระบบสารสนเทศภายในโรงพยาบาล ผลของการมีความเข้าใจและให้ความสำคัญในการรักษาความมั่นคงปลอดภัยสารสนเทศ นำไปสู่การเกิดเป็นทัศนคติที่ดี ซึ่งทัศนคตินั้นเป็นองค์ประกอบของแบบจำลองบันได 5 ขั้น โดย Khan et al. (2011) อธิบายได้ว่าการเกิดความตระหนักรู้เริ่มจากการมีความรู้ นำมาซึ่งทัศนคติความเชื่อผ่านสู่ความตั้งใจและการแสดงออกทางพฤติกรรมสอดคล้องกับผลการศึกษาที่ว่า บุคลากรของโรงพยาบาลศิครินทร์มีทัศนคติต่อการการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์ ปัจจัยดังกล่าวยังสอดคล้องกับงานวิจัยของ คณัสนันต์ ทองคำ (2561) ว่า ทัศนคติเกี่ยวกับความมั่นคงปลอดภัย ส่งผลต่อความตั้งใจในการปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร

4) ปัจจัยพฤติกรรมเชิงบวกที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์

จากการศึกษาพบว่าปัจจัยพฤติกรรมเชิงบวกที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ภาพรวมความคิดเห็นอยู่ในระดับน้อย ตีความได้ว่า บุคลากรของโรงพยาบาลมีพฤติกรรมการใช้งานระบบสารสนเทศโดยอาศัยความคุ้นเคยและเคยชินเป็นส่วนใหญ่ สะท้อนภาพว่า ผู้ตอบแบบสอบถามซึ่งส่วนใหญ่เป็นพยาบาลต้องใช้งานระบบสารสนเทศอยู่ตลอดเวลาเป็นส่วนใหญ่ทำให้จอคอมพิวเตอร์ในโรงพยาบาลแถบจะต้องเปิดอยู่ตลอดเวลาทำให้การปิดการใช้งาน (Log out) ทุกครั้ง เมื่อไม่ได้ใช้งานคอมพิวเตอร์ที่อยู่ในระบบสารสนเทศ และการพักหน้าจอ (Lockscreen) กับคอมพิวเตอร์ที่อยู่ในระบบสารสนเทศทุกครั้ง เมื่อไม่ได้อยู่ประจำคอมพิวเตอร์ปฏิบัติได้ยาก รวมถึงส่งข้อมูลสำคัญไม่ได้ส่งทางอีเมล์เท่านั้น สิ่งต่างๆ เหล่านี้สะท้อนให้เห็นว่า พฤติกรรมบางอย่างของบุคลากรของโรงพยาบาลเป็นช่องโหว่ของการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างหนึ่ง อย่างไรก็ตาม ผลการศึกษาพบว่า พฤติกรรมเชิงบวกยังส่งผลต่อลักษณะการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลศิครินทร์ สอดคล้องกับงานวิจัยของ วิไล ฤทธิเดช (2565) ที่พบว่า พฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศมีความสัมพันธ์เชิงบวกกับความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศ

ข้อเสนอแนะที่ได้รับจากการวิจัย

ข้อเสนอแนะเชิงนโยบาย 1) โรงพยาบาลศิครินทร์มีบุคลากรจำนวนมากซึ่งบุคลากรย่อมมีความแตกต่างทางด้านประชากรศาสตร์ ด้วยความแตกต่างเหล่านี้โรงพยาบาลไม่มีทางมั่นใจแน่ชัดว่าบุคลากรทุกท่านจะมีความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่เหมือนกัน ดังนั้นโรงพยาบาลควรกำหนดนโยบายเพื่อบริหารจัดการ

บุคลากรแต่ละท่านให้มีตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล 2) โรงพยาบาลศิครินทร์ควรทบทวนนโยบายเกี่ยวกับระบบสารสนเทศ เทคโนโลยีต่างๆ ที่ใช้งานภายในโรงพยาบาล 3) โรงพยาบาลศิครินทร์ควรกำหนดนโยบายเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลอย่างเป็นรูปธรรมตั้งแต่ระดับผู้บริหารถึงบุคลากรในทุกตำแหน่งงาน 3.1) การวางแผนเพื่อกำหนดวิสัยทัศน์ ยุทธศาสตร์ เป้าหมายที่มีต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล 3.2) กำหนดกรอบการศึกษาทบทวนความรู้เกี่ยวกับการสร้างความตระหนักรู้และการรักษาความมั่นคงปลอดภัยทางไซเบอร์ 3.3) จัดทำแผนปฏิบัติการให้สอดคล้องกับวิสัยทัศน์ ยุทธศาสตร์ เป้าหมายที่มีต่อการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล

ข้อเสนอแนะเชิงการบริหาร 1) ด้านบุคลากร โรงพยาบาลศิครินทร์ควรทำแผนพัฒนาบุคคลให้กับบุคลากรในโรงพยาบาลทุกระดับ เพื่อมั่นใจว่าบุคลากรมีความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล 1.1) ระดับผู้บริหารต้องเข้าใจ ตระหนักรู้ และส่งเสริมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล 1.2) ระดับบุคลากรอื่นๆ จัดทำระบบพัฒนาบุคลากรในแต่ละตำแหน่งงานโดยแยกบุคลากรที่ทำหน้าที่ดูแลและรับผิดชอบเกี่ยวกับระบบสารสนเทศของโรงพยาบาลพัฒนาให้เป็นผู้เชี่ยวชาญเพื่อให้มีความรู้ความสามารถในการใช้งาน ดูแล รักษา ปกป้องข้อมูลเกี่ยวกับระบบสารสนเทศของโรงพยาบาล ส่วนบุคลากรในตำแหน่งงานๆ อื่น ต้องได้รับการศึกษาทบทวนเกี่ยวความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล 2) ด้านงบประมาณ โรงพยาบาลศิครินทร์ควรทำแผนยุทธศาสตร์ แผนแม่บทและแผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล เมื่อมีแผนการต่างๆ ทำให้โรงพยาบาลสามารถจัดสรรงบประมาณอย่างมีประสิทธิภาพ 3) ด้านการบริหารจัดการ โรงพยาบาลศิครินทร์ควรมีการกำหนดการบริหารให้มีความชัดเจน ดังนี้ 3.1) สร้างระบบจัดการที่ดี โดยองค์กรควรยึดกรอบการปฏิบัติตามแผนยุทธศาสตร์ แผนแม่บทและแผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล 3.2) กระบวนการกำหนดความสำเร็จและความล้มเหลว เป็นการนำนโยบายขององค์กรมาทำให้เกิดประสิทธิผลโดยให้ความสำคัญกับการนำแผนต่างๆ มาปฏิบัติอย่างถูกต้องตามหลักการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล

ข้อเสนอแนะเชิงปฏิบัติการ 1) ด้านการวางแผน บุคลากรในโรงพยาบาลศิครินทร์ทุกระดับต้องปฏิบัติตามแผนยุทธศาสตร์ แผนแม่บทและแผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล เพื่อให้เป็นตามวิสัยทัศน์ขององค์กรเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ 2) ด้านการจัดการองค์กร โรงพยาบาลศิครินทร์ทำการจัดการบุคลากร โดยการมอบหมายหน้าที่ วิธีปฏิบัติเกี่ยวกับรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาลให้เหมาะสมกับแต่ละตำแหน่งงาน 3) ด้านการควบคุม โรงพยาบาลศิครินทร์ควรนำมาตรการ ข้อบังคับมาปฏิบัติพร้อมมีบทลงโทษ ตามกฎหมายและมาตรฐานสากลที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้บุคลากรของโรงพยาบาลปฏิบัติตามหลักการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศภายในโรงพยาบาล

ข้อเสนอแนะสำหรับการศึกษาครั้งถัดไป

1) งานวิจัยชิ้นนี้ไม่ได้ระบุให้บุคลากรในทุกสายงานที่มีในโรงพยาบาลร่วมตอบแบบสอบถาม ผู้สนใจที่จะทำการศึกษาวิจัยในรูปแบบของโรงพยาบาลหรือองค์กรควรเพิ่มเติมขอบเขตด้านประชากรในงานวิจัยให้ครอบคลุมและชัดเจน

2) งานวิจัยชิ้นนี้มีตัวแปรตาม 1 ตัว แต่มีองค์ประกอบ 4 มิติ ซึ่งเพื่อให้เกิดความชัดเจนมากยิ่งขึ้นควรที่จะวิเคราะห์องค์ประกอบทั้ง 4 มิติ เพิ่มเติม

3) งานวิจัยชิ้นนี้เป็นงานวิจัยเชิงปริมาณ เพื่อให้เกิดการออกแบบการตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่สมบูรณ์ครบถ้วนมากขึ้น เช่น เกิดรูปแบบการเรียนรู้และการฝึกอบรม รูปแบบของเครื่องมือและเทคโนโลยีที่

นำมาใช้ รูปแบบของนโยบายในองค์กร และรูปแบบของความร่วมมือในการปฏิบัติของบุคลากรในสายงานต่าง ๆ เห็นควรที่จะทำการศึกษาเนื้อหาต่าง ๆที่กล่าวมาในรูปแบบของงานวิจัยเชิงคุณภาพ

เอกสารอ้างอิง

กรรณิการ์ เหมือนประเสริฐ. (2548). *ทัศนคติของพนักงานที่มีความสัมพันธ์ต่อพฤติกรรมการปฏิบัติงานของพนักงานในองค์กรบริษัท คูเวต ปิโตรเลียม (ประเทศไทย) จำกัด*. ปริญญาบริหารธุรกิจมหาบัณฑิต, มหาวิทยาลัยศรีนครินทรวิโรฒ.

กิตติ ภักดีวัฒนะกุล และ พนิดา พานิชกุล. (2561). การพัฒนาระบบสารสนเทศเพื่อสนับสนุนการบริหารงานนโยบายและแผน มหาวิทยาลัยราชภัฏอุบลราชธานี. *วารสารวิชาการมหาวิทยาลัยการจัดการและเทคโนโลยีอีสเทิร์น, 15*(2), 255-265.

เกียรติศรี สำราญเวชพร. (2540). ระบบสารสนเทศย่อยมีการเชื่อมโยงกันภายในระบบสารสนเทศโรงพยาบาล. *วารสารรามาธิบดี*, 130-134.

คณัสนันต์ ทองคำ. (2561). *ปัจจัยที่ส่งผลต่อความตั้งใจของพนักงานในการปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบข้อมูลสารสนเทศในองค์กร กรณีศึกษา เทศบาลเมืองไร่ขิง อ.สามพราน จ.นครปฐม*. สาขาวิชานโยบายและการบริหารดิจิทัล, วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์.

ชยากร ทิพมาศ. (2565). *แนวทางการใช้เทคโนโลยีสารสนเทศในการบริหารสถานศึกษา สังกัดสำนักงานเขตพื้นที่การศึกษาประถมศึกษาพิจิตร เขต 1*. คณะศึกษาศาสตร์, มหาวิทยาลัยนเรศวร.

ชุมพล ศฤงคารศิริ. (2543). *การพัฒนาระบบสารสนเทศเพื่อสนับสนุนการประเมินผลการปฏิบัติราชการของบุคลากรสายวิชาการ*. คณะวิศวกรรมศาสตร์ สาขาวิชาเทคโนโลยีเพื่อสื่อสารการศึกษา, มหาวิทยาลัยมหาสารคาม.

ฐิติมา ภู่ห้อย. (2564). *การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์*. วิทยานิพนธ์ระดับปริญญาดุษฎีบัณฑิต, มหาวิทยาลัยศรีปทุม.

ธนพงศ์ ฉันทวิเชียร. (2566). *การพัฒนาระบบป้องกันและแจ้งเตือนภัยคุกคามทางไซเบอร์บนเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้เทคนิคการวิเคราะห์เหตุการณ์ตอบสนองต่อภัยคุกคามแบบเรียลไทม์*. สาขาวิชานิเทศศาสตร์การตลาด, มหาวิทยาลัยหอการค้าไทย.

พงศกร ทองพันธุ์. (2561). *แนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศ กลุ่มเครือข่ายบริการสุขภาพ อำเภอโคกศรีสุพรรณ จังหวัดสกลนคร*. วิทยานิพนธ์วิทยาศาสตรมหาบัณฑิต, มหาวิทยาลัยราชภัฏสกลนคร.

พรรณทิพา สาวันดี. (2554). *การศึกษาความตระหนักรู้ต่อการใช้อินเทอร์เน็ตอย่างสร้างสรรค์และปลอดภัยของนักเรียนชั้นประถมศึกษาปีที่ 5 โรงเรียนบ้านหนองน้ำขุ่น ที่เรียนด้วยบทเรียนคอมพิวเตอร์มัลติมีเดีย เรื่องทักษะการใช้อินเทอร์เน็ต*. สารนิพนธ์การศึกษามหาบัณฑิต, มหาวิทยาลัยศรีนครินทรวิโรฒ.

ภัทราวดี โศจิศรีสกุล. (2565). *ปัจจัยที่มีผลต่อการยอมรับและการนำระบบเทคโนโลยีสารสนเทศไปใช้งานของบุคลากรในส่วนงานการผลิต*. สารนิพนธ์การจัดการมหาบัณฑิต, มหาวิทยาลัยมหิดล.

มหาวิทยาลัยสุโขทัยธรรมาธิราช. (2562). *เอกสารการสอนชุดวิชาความมั่นคงปลอดภัยไซเบอร์ Cyber Security 99419 หน่วยที่ 1-5*.

วิมลพรรณ อาภาเวท และ ฉันทนา ปาปัดถา. (2554). การสร้างความรู้และความตระหนักในการเกิดอุบัติเหตุจากการฝ่าฝืนกฎจราจรของประชาชนในพื้นที่สถานีตำรวจภูธรเมืองนนทบุรี. *วารสารวิชาการคณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยราชภัฏเทพสตรี, 12*(1), 1-14.

วิไล ฤทธิเดช. (2565). *ความรู้ความตระหนักและพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากรสาธารณสุขในประเทศไทย กรณีศึกษาโรงพยาบาลพุทธโสธร*. วิทยานิพนธ์เภสัชศาสตรมหาบัณฑิต, มหาวิทยาลัยศิลปากร.

ศิริลักษณ์ เมธาธีระนันท์. (2562). *การศึกษาภัยคุกคามทางไซเบอร์จากช่องว่างระหว่างการวางนโยบายความปลอดภัยสารสนเทศกับการใช้งานจริงของพนักงานในองค์กร กรณีศึกษา บริษัทญี่ปุ่นในประเทศไทย*. การค้นคว้าอิสระวิทยาศาสตรมหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์.

สุขุม เฉลยทรัพย์ และคณะ. (2555). *หนังสือเรียนวิชาเทคโนโลยีสารสนเทศ, คณะมนุษยศาสตร์และสังคมศาสตร์*, มหาวิทยาลัยราชัฏสวนดุสิต.

สุธาเทพ รุณเรศ. (2561). *ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร*. การค้นคว้าอิสระวิทยาศาสตรมหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์.

อรรถพล กิตติธนาชัย. (2555). *พฤติกรรมการใช้เทคโนโลยีสารสนเทศที่สัมพันธ์ต่อสรรถนะของนักเรียนโรงเรียนสาธิตมหาวิทยาลัยศรีนครินทรวิโรฒประสานสิตร (ฝ่ายมัธยม)*. สารนิพนธ์การศึกษามหาบัณฑิต, มหาวิทยาลัยศรีนครินทรวิโรฒ.

Belani, G. (2020). *5 cybersecurity threats to be aware of in 2020*. Washington, DC: IEEE Computer Society.

Bélanger, F., Maier, J., & Maier, M. (2022). A longitudinal study on improving employee information protective knowledge and behaviors. *Computers & Security, 116*, 102641.

Buch, R., Ganda, D., Kalola, P., & Borad, N. (2017). World of cyber security and cybercrime. *Recent trends in programming languages, 4*(2), 18-23.

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.

Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., ... & Ntanos, C. (2022). A cybersecurity culture survey targeting healthcare critical infrastructures. *Healthcare, 10*(2), 327.

Hill, J. B., & Marion, N. E. (2016). *Introduction to cybercrime*. California: ABC -CLIO LLC.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International journal of information management, 45*, 13-24.

Lindau, K. (2012). *Cyber Security in Estonia: Lessons from the Year 2007 Cyberattack*. Master's thesis, Tallinn University.

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African journal of business management, 5*(26), 10862.

Tanner, A. (2015). *Gaining an Edge in Cyberspace with Advanced SituationalAwareness*. IBM Research.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Conflicts of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any

product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.



Copyright: © 2026 by the authors. This is a fully open-access article distributed under the terms of the Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).