ประสิทธิผลของการจัดการความปลอดภัยระบบสารสนเทศ โรงพยาบาลสระบุรี

Effectiveness of Information security Management in Saraburi Hospital

[1]สมศิริ พันธุ์ศักดิ์ศิริ และ [2*]เสาวนีย์ สมันต์ตรีพร

Somsiri Pansaksiri and Saowanee Samantreeporn

บัณฑิตวิทยาลัย มหาวิทยาลัยเอเชียอาคเนย์

Graduate School, Southeast Asia University, Thailand.

E-mail: [1]siri.pansaksiri@gmail.com, [2]film.phd5@gmail.com

*Corresponding Author

Received February 21, 2023; **Revised** April 21, 2023; **Accepted** April 24, 2023

บทคัดย่อ

บทความนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาอิทธิพลของความรู้ การตระหนักรู้ การจัดการ และพฤติกรรมการใช้สารสนเทศที่ส่งผลต่อประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศ โรงพยาบาลสระบุรี และ 2) สร้างแนวทางการปฏิบัติงานเพื่อความปลอดภัยของระบบสารสนเทศ งานวิจัยเป็นแบบผสานวิธี กลุ่มตัวอย่างเป็นบุคลากรของโรงพยาบาลสระบุรี แบ่งเป็น 2 กลุ่ม คือกลุ่มที่ 1 บุคลากรของโรงพยาบาลสระบุรี จำแนกตามสาขาวิชาชีพ จำนวน 317 คน ใช้วิธีการสุ่มแบบแบ่งชั้นแต่ละสาขาวิชาชีพ และกลุ่มที่ 2 เลือกแบบเฉพาะเจาะจงเป็นทีมผู้บริหารคุณภาพของโรงพยาบาลสระบุรี ซึ่งเป็นผู้ทำหน้าที่กำหนดทิศทางและนโยบายของโรงพยาบาลจำนวนทั้งหมดที่มีอยู่คือ 10 คน วิเคราะห์ข้อมูลโดยใช้สถิติเชิงพรรณนา หาความสัมพันธ์ด้วยการวิเคราะห์เส้นทาง และวิเคราะห์เนื้อหาจากการสนทนากลุ่มกับทีมผู้บริหารคุณภาพ

ผลวิจัยพบว่า ความรู้ การตระหนักรู้ การบริหารจัดการ และพฤติกรรมการใช้สารสนเทศ มีอิทธิพลทางตรงและทางอ้อม ต่อประสิทธิผลของการจัดการความปลอดภัยระบบสารสนเทศ โดยรูปแบบ ของโมเดลเส้นทางความสัมพันธ์มีความสอดคล้องกับข้อมูลเชิงประจักษ์ (Chi-square =142.41,df = 54, Chi-square/df= 2.63, GFI= 0.94, AGFI=0.90, CFI = 0.98 และ RMSEA = 0.07) โดยพบว่าการบริหารจัดการมีอิทธิพลต่อประสิทธิผลของการจัดการความปลอดภัยสารสนเทศมากที่สุด(1.040)รองมาคือ การตระหนักรู้ (0.540) ความรู้ด้านสารสนเทศและพฤติกรรมการใช้สารสนเทศ (0.220,0.081) ตามลำดับ โดยมีความสามารถในการทำนายร้อยละ 67 ผลของการสนทนากลุ่มพบว่าแนวทางการจัดการความปลอดภัยให้เกิดประสิทธิผล ต้องมีวิธีการวางแผน การบริหารจัดการ การ

ควบคุม กำกับ การจัดทำแนวทางการปฏิบัติ ซึ่งประกอบด้วยส่วนของผู้ดูแลระบบและส่วนของผู้ใช้งาน และต้องมีการปรับปรุงอย่างต่อเนื่อง

คำสำคัญ: ประสิทธิผลการจัดการความปลอดภัย; ระบบสารสนเทศ; โรงพยาบาลสระบุรี; Ransomware

Abstract

This article aimed to 1) study the influence of information literacy, security awareness, information management, and information usage behaviors on the effectiveness of information system security management at Saraburi Hospital, and 2) determine optimal operational guidelines for information system security. This research used an integrated approach, combining quantitative and qualitative methods. The population samples were personnel of Saraburi Hospital, divided into two groups. The first group contained 317 personnel of Saraburi Hospital classified by profession, obtained by stratified random sampling, and the second group contained 10 quality managers. The data were analyzed by descriptive statistics and path analysis of factors affecting the effectiveness of information security management and interpreted with a focus group discussion with the quality management team of Saraburi Hospital. The results are as follows:

Regarding level of knowledge, awareness, information management, information usage behavior and the effectiveness of information system management, opinions of all aspects were high and the path analysis of factors affecting the effectiveness of information security management was consistent with empirical data (Chi–square =142.41, df. = 54, Chi–square/df. = 2.63, GFI = 0.94, AGFI = 0.90, CFI = 0.98 and RMSEA = 0.07). Information management had the most influence on the effectiveness of information security management (1.040), followed by awareness (0.540), knowledge, and information usage behavior (0.220, 0.081), respectively. It was also found that information management, IT knowledge, and awareness indirectly influenced the effectiveness of information security management through information usage behavior, with 67% predictive power. The results of the focus group discussion showed that safety management was effective and that there must be a way of planning management, control, supervision, and the preparation of manuals as guidelines for information system practices. Guidelines must include administrator and user sections, direct performance control, and be constantly updated.

Keywords: Effectiveness; Information system; Saraburi Hospital; Ransomware

บทนำ

ความก้าวหน้าของเทคโนโลยีสารสนเทศ เป็นพลังที่ขับเคลื่อนสังคมที่นำไปสู่ภาคเศรษฐกิจ ธุรกิจ ทำให้เกิดการเปลี่ยนแปลงทางสิ่งแวดล้อม ประชากร เศรษฐกิจ สังคม และวัฒนธรรม (วศินี หนุนภักดี, 2562) เทคโนโลยีสารสนเทศและการสื่อสาร มีคุณประโยชน์หลากหลายประการและเป็นปัจจัยหลักในการพัฒนาประเทศ ช่วยสนับสนุนให้เกิดการพัฒนาทั้งด้านสังคม เศรษฐกิจ อุตสาหกรรม และการพัฒนาคุณภาพชีวิต การเผยแพร่ข้อมูลข่าวสาร การประชาสัมพันธ์และการติดต่อสื่อสาร เกิดการเปลี่ยนแปลง เกิดการเคลื่อนย้ายอย่างรวดเร็ว (Hong et al., 2018) การพัฒนาเทคโนโลยีสื่อสารและสารสนเทศ ส่งผลให้โลกมีสภาพ เหมือนเป็นหนึ่งเดียว เกิดการแข่งขันในวงกว้าง แนวโน้มการพัฒนาเป็นไปทั้งทางด้านบวกและด้านลบ ในด้านบวกคือการพัฒนาเครือข่ายคอมพิวเตอร์ และเครือข่ายอินเทอร์เน็ตที่เชื่อมโยงกันทั่วโลก ก่อให้เกิดการเปลี่ยนแปลงทางสังคม ช่องทางการดำเนินธุรกิจ การพัฒนาระบบสารสนเทศ ฐานข้อมูล ฐานความรู้ เพื่อการจัดการความรู้ การศึกษาตามอัธยาศัยด้วยระบบอิเล็กทรอนิกส์ (e-learning) การเรียนการสอนด้วยระบบโทรศึกษา (tele-education) การค้นคว้าหาความรู้ได้ตลอด 24 ชั่วโมงจากห้องสมุดเสมือน (virtual library) การบริหารจัดการภาครัฐสมัยใหม่ โดยการใช้เทคโนโลยีสารสนเทศและเครือข่ายการสื่อสารเพื่อเพิ่มประสิทธิภาพการดำเนินการของภาครัฐที่เรียกว่า รัฐบาลอิเล็กทรอนิกส์ (e-government) รวมทั้งระบบฐานข้อมูลประชาชน (e-citizen) สำหรับในด้านลบ เกิดความผิดพลาดในการทำงานของระบบคอมพิวเตอร์ ทั้งส่วนฮาร์ดแวร์และซอฟต์แวร์ จากการออกแบบและพัฒนา ทำให้เกิดความเสียหายต่อระบบและสูญเสียค่าใช้จ่ายในการแก้ปัญหา การละเมิดลิขสิทธิ์ของทรัพย์สินทางปัญญา การทำสำเนาและลอกเลียนแบบ การก่ออาชญากรรมทางคอมพิวเตอร์ การโจรกรรมข้อมูล การเข้ารหัสข้อมูล และการก่อกวนระบบคอมพิวเตอร์ สิ่งเหล่านี้ย่อมส่งผลเสียต่อผู้ใช้งานเมื่อผู้ใช้งานขาดความรู้ในการป้องกันตนเองอย่างเหมาะสม อาจเป็นเหตุนำมาซึ่งความเสื่อมเสียต่อตนเองทั้งข้อมูลและทรัพย์สิน (อนันต์ ชูยิ่งสกุลทิพย์, 2562) องค์กรในระบบการให้บริการด้านสุขภาพหลายแห่งทั้งภาครัฐและเอกชนในประเทศไทยได้มีความพยายามที่จะเปลี่ยนระบบการจัดเก็บข้อมูล จากการใช้ระบบการบันทึกบนกระดาษมาเป็นระบบเอกสารอิเล็กทรอนิกส์เพื่อลดปัญหาด้านการสื่อสาร การจัดเก็บ การสูญหายของเอกสาร ง่ายต่อการสืบค้นข้อมูล และลดการสิ้นเปลืองทรัพยากรกระดาษ การปรับตัวเพื่อยอมรับและเรียนรู้เทคโนโลยีใหม่ๆที่เกิดขึ้นโดยเฉพาะระบบข้อมูลและการบริหารจัดการข้อมูลที่ดี จะสามารถสร้างความได้เปรียบและนำไปสู่ความสำเร็จในอนาคตได้ (อดิศักดิ์ ถิระแก้ว และ ปุญชรัศมิ์ ศักดิ์ธรรมเจริญ, 2561)

โรงพยาบาลสระบุรี ได้มีการพัฒนาเทคโนโลยีสารสนเทศมาอย่างต่อเนื่องเพื่อรองรับการให้บริการผู้ป่วยโดยเฉลี่ยวันละ 3,000 คน โดยพัฒนาเป็นระบบ เวชระเบียนอิเล็กทรอนิกส์ (Electronic Medical Record) มีฐานข้อมูลการรักษาพยาบาลที่มีคุณภาพ สามารถเรียกดูหรือประมวลผลข้อมูลเพื่อนำมาใช้ในการวางแผนการปฏิบัติงานได้ แบบอัตโนมัติ (real time) (สมศิริ พันธุ์ศักดิ์ศิริ, 2562) สำหรับ

ด้านคุณภาพของเทคโนโลยีสารสนเทศได้กำหนดแนวทางการปฏิบัติงาน ตามมาตรฐานของ Healthcare Accreditation Information Technology: HAiT (ชุษณะ มกรสาร และ วรรษา เปาอินทร์, 2561) ภาวะวิกฤตเกิดขึ้นเมื่อโรงพยาบาลสระบุรี ถูกจารกรรมระบบคอมพิวเตอร์ ด้วยการส่งไวรัส Ransomware เข้ารหัสข้อมูลเพื่อเรียกค่าไถ่ เข้าสู่ระบบคอมพิวเตอร์ ทำให้โรงพยาบาลเกิดภาวะวิกฤตอย่างมาก ส่งผลให้ฐานข้อมูลผู้ป่วย และระบบเครือข่าย ไม่สามารถใช้งานได้ ความรุนแรงจากแรนซัมแวร์หรือมัลแวร์เรียกค่าไถ่ เป็นมัลแวร์ที่ไม่ให้ผู้ใช้งานเข้าถึงไฟล์หรือระบบของตน และให้ชำระเงินเป็นดิจิทัลเพื่อถอดรหัสแล้วจึงส่งไฟล์กลับไปยังผู้ใช้อีกครั้ง แรนซัมแวร์ประเภทนี้เป็นอันตรายเนื่องจากโจมตีไฟล์ทั้งหมดและยากที่จะหาวิธีป้องกัน (Chesti et al., 2020)

ความสูญเสียที่เกิดขึ้น ส่งผลให้โรงพยาบาลสระบุรี ประสบปัญหาทางด้านการเข้าถึงข้อมูลผู้ป่วย และระบบเครือข่าย ความสูญเสียด้านการเงินของโรงพยาบาลสระบุรีในช่วงเวลาที่เกิดวิกฤตเทียบกับช่วงเวลาเดียวกันของปีก่อนเกิดภาวะวิกฤติ และปีถัดมาหลังเกิดภาวะวิกฤต พบว่าโรงพยาบาลสระบุรี สูญเสียรายได้ที่เก็บข้อมูลจากการให้บริการตรวจรักษาจากผู้ป่วยนอกและผู้ป่วยในลดลงอย่างมาก จากในช่วงเดือนกันยายน ของปี 2562 ถึงปี 2564 การรับรู้รายได้จากการให้บริการตรวจรักษาพยาบาล ทั้งผู้ป่วยนอกและผู้ป่วยที่รับไว้รักษาในโรงพยาบาล ในปี 2562 เป็นจำนวนเงิน 100,609,331 บาท ส่วนปี 2563 ช่วงเวลาเกิดภาวะวิกฤต รับรู้รายได้ลดลงเหลือ 32,226,711 บาท และในปี 2564 รับรู้รายได้เป็นจำนวนเงิน 171,721,044 บาท (โรงพยาบาลสระบุรี, 2565) ทำให้รายได้ที่ได้รับจากกองทุนที่ส่งข้อมูลเพื่อเรียกเก็บค่ารักษาพยาบาล เพื่อนำมาใช้ในการบริหารจัดการ การจัดหาวัสดุอุปกรณ์ การให้บริการและการดูแลรักษาผู้ป่วยลดลง ผลการวิเคราะห์สถานการณ์ เพื่อหาสาเหตุของการเกิดภาวะวิกฤต ระบบสารสนเทศของโรงพยาบาลสระบุรี (สมศิริ พันธุ์ศักดิ์ศิริ และเสาวนีย์ สมันต์ตรีพร, 2565) พบว่า ปัจจัยเสี่ยงที่ทำให้เกิด Ransomware incidence มาจากเจ้าหน้าที่ที่เกี่ยวข้อง ขาดความรู้ ความเข้าใจ ความตระหนัก และพฤติกรรมในเรื่องของความเสี่ยงและความปลอดภัยของสารสนเทศ การมีระบบเครือข่ายที่เน้นความสะดวกในการใช้งานโดยไม่ได้มีการควบคุมพฤติกรรมการใช้งาน และระบบการสำรองข้อมูลยังไม่ดีพอ จึงเป็นสิ่งจำเป็นอย่างยิ่งที่ต้องหาวิธีการให้ระบบสารสนเทศของโรงพยาบาลสระบุรีมีความปลอดภัย โดยสร้างความรู้ความเข้าใจ การตระหนักรู้ในการใช้งานสารสนเทศ และสร้างพฤติกรรมการใช้สารสนเทศที่เหมาะสม เพื่อให้เกิดประสิทธิผลในอนาคต ผลที่ได้นอกจากจะก่อให้เกิดประโยชน์กับโรงพยาบาลสระบุรีแล้ว แนวทางการแก้ปัญหาเพื่อให้เกิดความมั่นคง ปลอดภัยด้านสารสนเทศและแนวทางการปฏิบัติที่เหมาะสมจะเป็นประโยชน์อย่างยิ่งสำหรับเศรษฐกิจและสังคมโดยรวมต่อไป

วัตถุประสงค์การวิจัย

1. เพื่อศึกษาอิทธิพลของความรู้ด้านสารสนเทศ การตระหนักรู้ การจัดการสารสนเทศ และพฤติกรรมการใช้งานสารสนเทศที่มีต่อประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศ โรงพยาบาลสระบุรี

2. สร้างแนวทางในการปฏิบัติงานเพื่อสร้างความปลอดภัยของระบบสารสนเทศ โรงพยาบาลสระบุรี

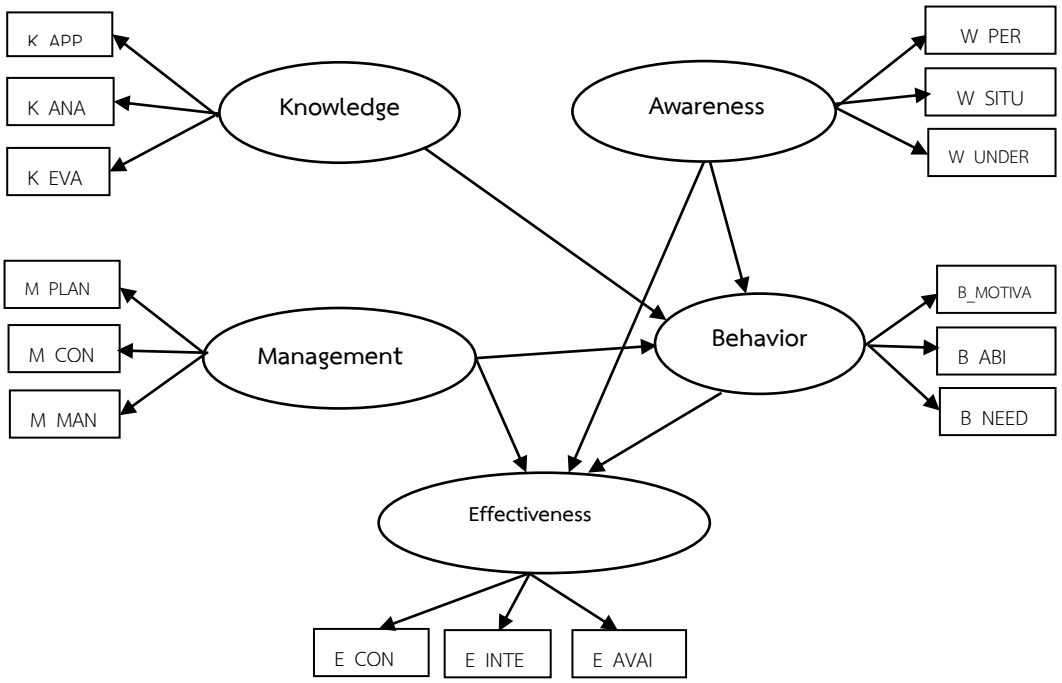
การทบทวนวรรณกรรม

การศึกษานี้เป็นการหาแนวทางเพื่อให้เกิดประสิทธิผลต่อความปลอดภัยระบบสารสนเทศ โรงพยาบาลสระบุรี ผู้วิจัยได้ศึกษาแนวคิดและทฤษฎีที่เกี่ยวข้องโดยครอบคลุมรายละเอียดเกี่ยวกับประสิทธิผลการจัดการความปลอดภัยของระบบสารสนเทศ (Gross, 1972) มีการใช้ทรัพยากรได้อย่างคุ้มค่า องค์กรมีกลไกที่สามารถปรับเปลี่ยนการดำเนินงานให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลง สามารถเพิ่มศักยภาพ (Potential) และความสามารถ (Capacity) ขององค์กรให้เจริญก้าวหน้าจึงนับว่ามีการทำงานที่มีประสิทธิผล (Schermerhorn et al., 1991) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transactions Development Agency :Thai CERT) ได้กำหนดแนวคิดของประสิทธิผลความปลอดภัยของระบบสารสนเทศ ขึ้นเรียกว่า C.I.A Triangle ประกอบด้วย การรักษาความลับ (Confidentiality) ความครบถ้วนสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) โดยแนวคิดและทฤษฎีที่เกี่ยวข้องกับความปลอดภัยของสารสนเทศ ประกอบด้วย ความรู้ด้านสารสนเทศ (Information Literacy) ซึ่งเป็นความสามารถในการเข้าถึงสารสนเทศ การประเมินผล การบริหารจัดการและการใช้สารสนเทศจากแหล่งต่างๆ สามารถค้นหาสารสนเทศที่ต้องการเพื่อการทำงานหรือการตัดสินใจในสิ่งที่เกิดขึ้นหรือการใช้สารสนเทศอย่างมีประสิทธิภาพ (Bloom, 1956) ระบบสารสนเทศนอกจากจะเป็นเรื่องของข้อมูลแล้วผู้ใช้งานต้องมีความรู้ ซึ่งสองส่วนนี้ต้องมีความเชื่อมโยงกันเพื่อการใช้สารสนเทศที่ถูกต้องและปลอดภัย (Edwards, 2022) ผู้ใช้งานต้องมีความตระหนักรู้เกี่ยวกับความปลอดภัยของสารสนเทศคือต้องมีการสร้างการรับรู้ ความเข้าใจและการวิเคราะห์สถานการณ์ ด้านการรักษาความมั่นคงปลอดภัยให้กับบุคลากรในองค์กร เพื่อให้บุคลากรมีพฤติกรรมที่สามารถดูแลรักษาและใช้งานทรัพยากรสารสนเทศขององค์กรได้อย่างปลอดภัย โรงพยาบาลสระบุรีพบกับอุปสรรคและความท้าทายอย่างมาก เมื่อถูกไวรัส Ransomware โจมตีด้วยการเข้ารหัส (Encrypted) ทำให้ฐานข้อมูลที่มีอยู่ไม่สามารถเข้าใช้งานได้ เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ โรงพยาบาลสระบุรีที่มีอยู่ไม่มีความชำนาญ มีความรู้และความเชี่ยวชาญไม่มากพอที่จะดำเนินการแก้ไข ต้องขอความช่วยเหลือไปยังผู้เชี่ยวชาญที่ ศูนย์ไซเบอร์กองทัพอากาศ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ศูนย์ประสานความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ประเทศไทย (Thailand Computer Emergency Response Team : Thai CERT) และคณะกรรมการไซเบอร์แห่งชาติ เพื่อช่วยคลี่คลายสถานการณ์

จนกระทั่งกลับมาเป็นปกติ และเสนอให้โรงพยาบาลสระบุรี ออกนโยบายองค์กรมุ่งเน้น ในส่วนของการบริหารจัดการสารสนเทศ (อานนท์ ไทยเจริญ และ สมศิริ พันธุ์ศักดิ์ศิริ, 2564) สนับสนุนทฤษฎีเกี่ยวกับการจัดการสารสนเทศ ของ Fayol (1964) ซึ่งประกอบด้วย การวางแผน (Planning) การบริหารจัดการจัดองค์กร (Organizing) การบังคับบัญชาสั่งการ (Commanding) การประสานงาน (Coordination) และการควบคุม (Controlling) โดยการจัดการด้านเทคโนโลยีสารสนเทศเพื่อสนับสนุนกระบวนการทำงานของบุคลากรในองค์กรให้มีพฤติกรรมการใช้สารสนเทศที่เหมาะสม สามารถนำสารสนเทศที่มีคุณภาพ ไปใช้ให้เกิดเป็นประโยชน์อย่างยิ่งในการบริหารงานและจัดการด้านการเงินการคลัง และประชาชนผู้รับบริการของโรงพยาบาลสระบุรี

กรอบแนวคิดการวิจัย

การวิจัยนี้ผู้วิจัยกำหนดกรอบแนวคิดประสิทธิผลการจัดการความปลอดภัยของระบบสารสนเทศ ตามแนวคิดสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transactions Development Agency :Thai CERT) ทฤษฎีของ Bloom (1956) ทฤษฎีเกี่ยวกับการจัดการสารสนเทศของ Fayol (1964) และงานวิจัยที่เกี่ยวข้อง แสดงความสัมพันธ์ของตัวแปรดังภาพที่ 1



ภาพที่ 1 ตัวแบบปัจจัยเชิงสาเหตุที่มีอิทธิพลต่อประสิทธิผลของการจัดการความปลอดภัยของระบบสารสนเทศ

สมมติฐานการวิจัย

H1. ความรู้ด้านสารสนเทศส่งผลต่อประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศ

H2. ความตระหนักรู้สารสนเทศส่งผลต่อประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศ

H3. การจัดการสารสนเทศส่งผลต่อประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศ

H4. พฤติกรรมการใช้สารสนเทศส่งผลต่อประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศ

H5. ความรู้ด้านสารสนเทศ การตระหนักรู้สารสนเทศ และการจัดการสารสนเทศ ส่งผลทางตรงและทางอ้อมต่อประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศผ่านพฤติกรรมการใช้สารสนเทศ

ระเบียบวิธีวิจัย

การวิจัยนี้เป็นงานวิจัยแบบผสมวิธี (Mixed methods research) มีรายละเอียดดังนี้

งานวิจัยเชิงปริมาณ

ประชากร (Population) คือบุคลากรของโรงพยาบาลสระบุรี คำนวณตัวอย่างโดยใช้โปรแกรม G*Power 3.1.9.4 กำหนด พารามิเตอร์ที่ใช้ในการคำนวณคือ Effect size ของการทดสอบอิทธิพลของตัวแปร เท่ากับ 0.40 (นิพิฐพนธ์ สนิทเหลือ และคณะ, 2562; Cohen, 1992) ความน่าจะเป็นของความคลาดเคลื่อน(Error Probability)เท่ากับ 0.05 อำนาจการทดสอบ (Power of test) เท่ากับ 0.85 และ Degree of freedom (Df.) เท่ากับ 120 ได้จำนวนตัวอย่าง (n) เท่ากับ 317 คน สุ่มตัวอย่างแบบแบ่งชั้น (Stratified random sampling) การเก็บตัวอย่างกระจายตามสัดส่วนของประชากรในแต่ละกลุ่ม (ภิรมย์ กมลรัตนกุล, 2550) จำนวนตัวอย่างที่ได้คือกลุ่มแพทย์ ทันตแพทย์ จำนวน 38 คน เภสัชกร จำนวน 10 คน พยาบาลวิชาชีพ จำนวน 128 คน นักวิชาการ จำนวน 21 คน และบุคลากรสาขาอื่นที่เกี่ยวข้องกับการใช้งานสารสนเทศ จำนวน 120 คน วิธีการได้มาของตัวอย่างแต่ละกลุ่มใช้วิธีการจับฉลากจากรหัสพนักงานแต่ละสาขาวิชาชีพ เพื่อให้เป็นตัวแทนของบุคลากรโรงพยาบาลสระบุรี

เครื่องมือที่ใช้ในการวิจัย การวิจัยเชิงปริมาณผู้วิจัยใช้แบบสอบถาม ที่ทดสอบดัชนีความสอดคล้อง (Index Item objective Congruence :IOC) มีค่าอยู่ระหว่าง 0.60–1.00 และค่าความเชื่อมั่นของครอนบาค (Cronbach) ได้ค่าเท่ากับ 0.93 เก็บรวบรวมข้อมูลโดยกระจายตามสัดส่วนของจำนวนตัวอย่างที่คำนวณได้ โดยส่งแบบสอบถามไปยังทุกหน่วยงานที่มีผู้ถูกสุ่มเลือกเป็นตัวอย่างปฏิบัติอยู่แล้วเก็บกลับคืนด้วยตนเอง แบบสอบถามในการเก็บรวบรวมข้อมูล แบ่งเป็น 4 ส่วน ดังนี้

ส่วนที่ 1 ข้อมูลทั่วไปประกอบด้วย เพศ อายุ ตำแหน่ง การศึกษา ประสบการณ์การใช้สารสนเทศ และการใช้ประโยชน์จากสารสนเทศที่มีในระบบ

ส่วนที่ 2 ความคิดเห็นของผู้ใช้บริการที่มีต่อความปลอดภัยของระบบสารสนเทศ ประกอบด้วย ความรู้ด้านสารสนเทศ การตระหนักรู้ การบริหารจัดการ และพฤติกรรมการใช้สารสนเทศ

ส่วนที่ 3 ประสิทธิผลของการจัดการความปลอดภัยระบบสารสนเทศโรงพยาบาลสระบุรี

ส่วนที่ 4 ข้อเสนอแนะเพื่อการพัฒนาระบบฯ

การวิเคราะห์ข้อมูล

ข้อมูลที่เก็บรวบรวมจากแบบสอบถามนำมาวิเคราะห์แบ่งเป็น สถิติเชิงพรรณนาสำหรับข้อมูลคุณลักษณะทางประชากร และปัจจัยเกี่ยวกับความรู้ด้านสารสนเทศ การตระหนักรู้สารสนเทศ การบริหารจัดการสารสนเทศ พฤติกรรมการใช้งานสารสนเทศ และประสิทธิผลของการจัดการความปลอดภัยของสารสนเทศ นำเสนอในรูปแบบของค่าร้อยละ ค่าเฉลี่ยและ ค่าเบี่ยงเบนมาตรฐาน และทดสอบสมมติฐานเพื่อศึกษาอิทธิพลของความรู้ด้านสารสนเทศ การตระหนักรู้ การจัดการสารสนเทศ และพฤติกรรมการใช้งานสารสนเทศที่มีต่อประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศ โดยการวิเคราะห์เส้นทางความสัมพันธ์ (Path Analysis)

การวิจัยเชิงคุณภาพ

ผู้ให้ข้อมูลหลัก(key informant) เลือกแบบเฉพาะเจาะจง (Purposive Sampling) โดยเป็นผู้บริหารที่มีบทบาทในการกำหนดนโยบายและทิศทางเพื่อขับเคลื่อนองค์กร คือทีมบริหารคุณภาพ (Quality Steering Team : QST) ซึ่งมีจำนวนทั้งหมด 10 คน โดยเก็บข้อมูลกับผู้บริหารทุกคน ซึ่งประกอบด้วย ผู้อำนวยการโรงพยาบาล รองผู้อำนวยการฝ่ายการแพทย์คนที่ 1 รองผู้อำนวยการฝ่ายการแพทย์คนที่ 2 รองผู้อำนวยการระบบบริการสุขภาพ รองผู้อำนวยการฝ่ายบริหาร รองผู้อำนวยการฝ่ายการพยาบาล ผู้ช่วยผู้อำนวยการด้านหลักประกันสุขภาพ ผู้ช่วยผู้อำนวยการด้านเทคโนโลยีสารสนเทศ ผู้ช่วยผู้อำนวยการด้านเวชระเบียนและสถิติและหัวหน้ากลุ่มงานเภสัชกรรม ผู้วิจัยกำหนดวัน เวลา และสถานที่ในการสนทนากลุ่ม (focus group)

เครื่องมือที่ใช้ในการวิจัย ในการเก็บรวบรวมข้อมูล ใช้ข้อคำถามปลายเปิดในการสนทนา โดยมีประเด็นการสนทนาเกี่ยวกับความรู้ การตระหนักรู้ การบริหารจัดการสารสนเทศ และพฤติกรรมการใช้สารสนเทศ ของบุคลากรโรงพยาบาลสระบุรี รวบรวมข้อมูลโดยนัดหมาย กำหนดวันเวลา และสถานที่ในการประชุมกลุ่ม ผู้วิจัยสร้างบรรยากาศ เพื่อให้ทีมเห็นถึงความมุ่งมั่นและความตั้งใจที่จะนำผลที่ได้จากการสนทนาไปเป็นแนวทางการสร้างความปลอดภัยให้ระบบสารสนเทศ เปิดโอกาสให้ผู้เข้าร่วมสนทนาทุกคนแลกเปลี่ยนความคิดเห็นและข้อเสนอแนะ เมื่อพูดคุยจนครบประเด็น และพบว่าไม่มีประเด็นข้อเสนอใหม่จึงยุติการสนทนา

การวิเคราะห์ข้อมูล

วิเคราะห์ข้อมูลเชิงคุณภาพเป็นการวิเคราะห์แบบเรียบเรียงพรรณนา นำข้อมูลที่ได้จากการสนทนากลุ่ม จัดเรียบเรียง และเลือกข้อความที่บ่งบอกถึงความสัมพันธ์ของตัวแปร การสรุป/การตีความด้วยวิธีการวิเคราะห์เนื้อหา (content Analysis)

ผลการวิจัย

ข้อมูลคุณลักษณะทางประชากร

พบว่า กลุ่มตัวอย่างส่วนใหญ่เป็นเพศหญิง คิดเป็นร้อยละ 91.80 อายุอยู่ในช่วง 31–40 ปี ร้อยละ 29.10 ส่วนมากเป็นพยาบาลวิชาชีพ ร้อยละ 40.40 ระดับการศึกษาพบว่า ร้อยละ 71.30 จบการศึกษาในระดับปริญญาตรี บุคลากรส่วนใหญ่มีประสบการณ์ในการใช้เทคโนโลยีสารสนเทศมากกว่า 10 ปีร้อยละ 67.80 สำหรับการใช้งานในระบบสารสนเทศ พบว่า ส่วนใหญ่ใช้เพื่อการบันทึกข้อมูล ร้อยละ 92.40 สำหรับการบริหารจัดการข้อมูล และการตรวจสอบข้อมูล ใช้เพียงร้อยละ 14.50 และ 10.10 ตามลำดับ ส่วนการนำข้อมูลในระบบมาใช้ พบว่า มีการนำข้อมูลมาใช้ในการวางแผนพัฒนางาน ร้อยละ 40.40 รองลงมาเป็นการนำมาใช้เพื่อวิเคราะห์เพื่อใช้ศึกษาปัญหา/สถานการณ์ ร้อยละ 29.30 และในเรื่องของการนำไปใช้เพื่อรายงานผลการปฏิบัติงานและใช้เพื่อการศึกษาวิจัยมีเพียงร้อยละ 24.10 และร้อยละ 13.90 ตามลำดับ

ผลการวิเคราะห์ปัจจัย

ความรู้ด้านสารสนเทศ การตระหนักรู้สารสนเทศ การบริหารจัดการสารสนเทศ พฤติกรรมการใช้งานสารสนเทศ และประสิทธิผลของการจัดการความปลอดภัยของระบบสารสนเทศ ของบุคลากรโรงพยาบาลสระบุรี โดยแบ่งรู้ด้านสารสนเทศแบ่งเป็น 3 ประเด็นย่อยคือ การประยุกต์ใช้ความรู้ การประเมินผล และการวิเคราะห์สารสนเทศ ด้านการตระหนักรู้สารสนเทศแบ่งเป็น 3 ประเด็นย่อยคือ การรับรู้สารสนเทศ ความเข้าใจ และการวิเคราะห์สถานการณ์ การบริหารจัดการสารสนเทศแบ่งเป็น 3 ประเด็นย่อย คือการวางแผน การจัดการ และการควบคุมกำกับ สำหรับด้านพฤติกรรมการใช้งานสารสนเทศ แบ่งเป็น 3 ประเด็นย่อย คือ การตอบสนองความต้องการ การจูงใจในการใช้งานและความสามารถในการใช้สารสนเทศ และด้านประสิทธิผลของการจัดการความปลอดภัยของสารสนเทศ โดยศึกษาประเด็นย่อยที่สำคัญ 3 ประเด็น คือ การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วนสมบูรณ์ (Integrity) และความพร้อมใช้ (Availability) รายละเอียดดังตารางที่ 1

ตารางที่ 1 ค่าเฉลี่ย ค่าส่วนเบี่ยงเบนมาตรฐานและระดับของความรู้ การตระหนักรู้ การบริหารจัดการ พฤติกรรมการใช้สารสนเทศ และประสิทธิผลของการจัดการระบบสารสนเทศ

ตัวแปร	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	CV	ระดับ
ความรู้ สารสนเทศ	4.28	0.48	0.112	มาก
การตระหนักรู้สารสนเทศ	3.86	0.43	0.111	มาก
การบริหารจัดการสารสนเทศ	3.93	0.45	0.115	มาก
พฤติกรรมการใช้สารสนเทศ	3.72	0.39	0.105	มาก
ประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศ	4.05	0.54	0.133	มาก

จากตารางพบว่า ปัจจัยที่มีส่วนเกี่ยวข้องกับประสิทธิผลของการจัดการระบบสารสนเทศ ทุกประเด็นมีค่าเฉลี่ยอยู่ในระดับมากโดยเฉพาะ ในเรื่องความรู้ระบบสารสนเทศมีค่าเฉลี่ยเท่ากับ 4.28 ค่าสัมประสิทธิ์ความแปรผัน ร้อยละ 11.20 ซึ่งแสดงให้เห็นว่ากลุ่มตัวอย่างมีการตอบข้อคำถามในเรื่องของความรู้ระบบสารสนเทศ ค่อนข้างเป็นไปในทิศทางเดียวกัน

การวิเคราะห์อิทธิพลของความรู้ด้านสารสนเทศ การตระหนักรู้ การจัดการสารสนเทศ และพฤติกรรมการใช้งานสารสนเทศที่มีต่อประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศโรงพยาบาลสระบุรี

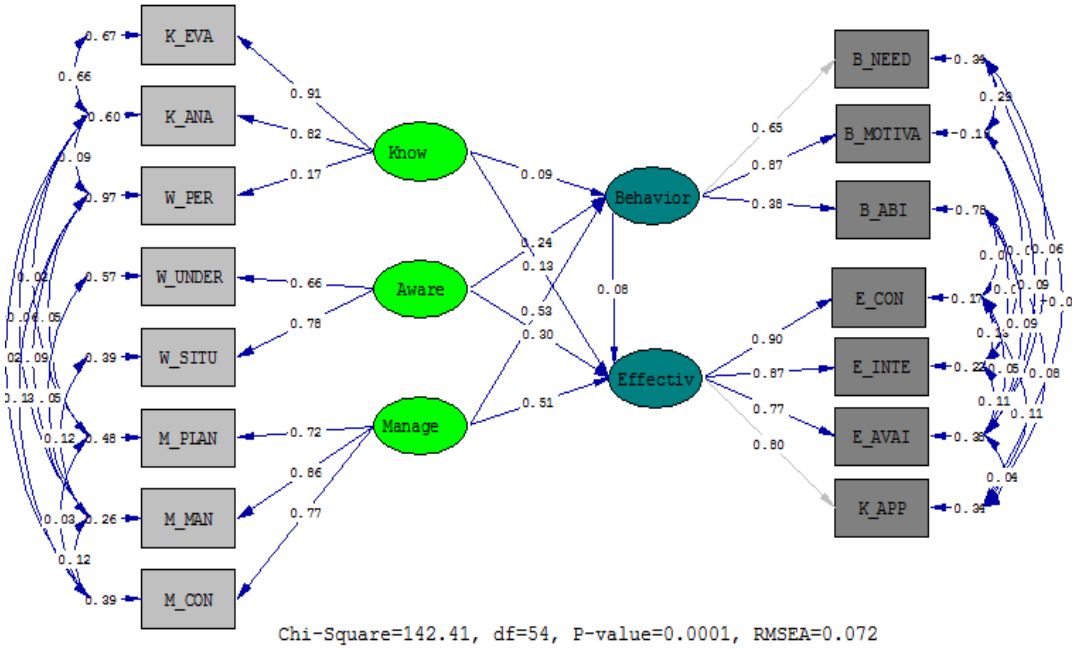
การวิเคราะห์อิทธิพลของความรู้ด้านสารสนเทศ การตระหนักรู้ การจัดการสารสนเทศ และพฤติกรรมการใช้งานสารสนเทศที่มีต่อประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศโรงพยาบาลสระบุรี เป็นการศึกษาความสัมพันธ์ โดยใช้ค่า KMO และค่า Bartlett test พบว่าค่า KMO ในภาพรวมเท่ากับ 0.89 ซึ่งมากกว่า 0.60 แสดงว่าตัวแปรทั้งหมดมีความสัมพันธ์กัน ค่า Bartlett' s test Sphericity มีค่าไคสแควร์เท่ากับ 2751.33 และ p-value =0.000 ซึ่งน้อยกว่าระดับนัยสำคัญ 0.05 แสดงว่าตัวแปรทั้งหมดไม่เป็นอิสระต่อกันหรือมีความสัมพันธ์กัน และเมื่อนำตัวแปรมาทดสอบความสัมพันธ์ด้วยสถิติ Pearson coefficient correlation พบว่า ตัวแปรทั้งหมดมีความสัมพันธ์กันจึงสามารถนำมาวิเคราะห์องค์ประกอบและตัวแบบสมการโครงสร้างได้ จากนั้นทำการตรวจสอบความสอดคล้องของตัวแบบ พบว่า ตัวแบบมีความสอดคล้องและกลมกลืนกับข้อมูลเชิงประจักษ์ หลังจากปรับตัวแบบ รายละเอียดดังเมทริกซ์สหสัมพันธ์ ตารางที่ 2 และตัวแบบปัจจัยเชิงสาเหตุภาพที่ 3

ตารางที่ 2 เมทริกซ์สหสัมพันธ์ของปัจจัยที่ส่งผลต่อประสิทธิผลของการจัดการความปลอดภัยระบบสารสนเทศ

Valiable	Correlation														
	K_APP	K_ANA	K_VEA	W_PER	W_UNDER	W_SITU	M_PLAN	M_MAN	M_CON	B_NEED	B_MOTIVA	B_ABI	E_CON	E_INTE	E_AVAI
K_APP	1	0.555**	.457**	0.399**	0.322**	0.492**	0.368**	0.453**	0.443**	0.308**	0.494**	0.297**	0.633**	0.718**	0.679**
K_ANA		1	0.819**	0.241**	0.432**	0.494**	0.397**	0.498**	0.384**	0.279**	0.504**	0.206**	0.647**	0.550**	0.510**
K_VEA			1	0.304**	0.411**	0.499**	0.368**	0.383**	0.327**	0.282**	0.479**	0.240**	0.571**	0.467**	0.440**
W_PER				1	0.181**	0.174**	0.225**	0.227**	0.118*	0.256**	0.122*	0.282**	0.121*	0.118*	0.246**
W_UNDER					1	0.513**	0.244**	0.332**	0.243**	0.171**	0.369**	0.207**	0.401**	0.305**	0.283**
W_SITU						1	0.301**	0.463**	0.272**	0.263**	0.362**	0.299**	0.463**	0.458**	0.381**
M_PLAN							1	0.624**	0.585**	0.426**	0.413**	0.164**	0.464**	0.498**	0.377**
M_MAN								1	0.584**	0.420**	0.495**	0.205**	0.558**	0.624**	0.555**
M_CON									1	0.394**	0.432**	0.131*	0.519**	0.555**	0.476**
B_NEED										1	0.600**	0.397**	0.341**	0.364**	0.377**
B_MOTIVA											1	0.512**	0.530**	0.469**	0.599**
B_ABI												1	0.270**	0.269**	0.203**
E_CON													1	0.679**	0.671**
E_INTE														1	0.700**
E_AVAI															1

**Correlation is significant at the 0.01 level (2-tailed)

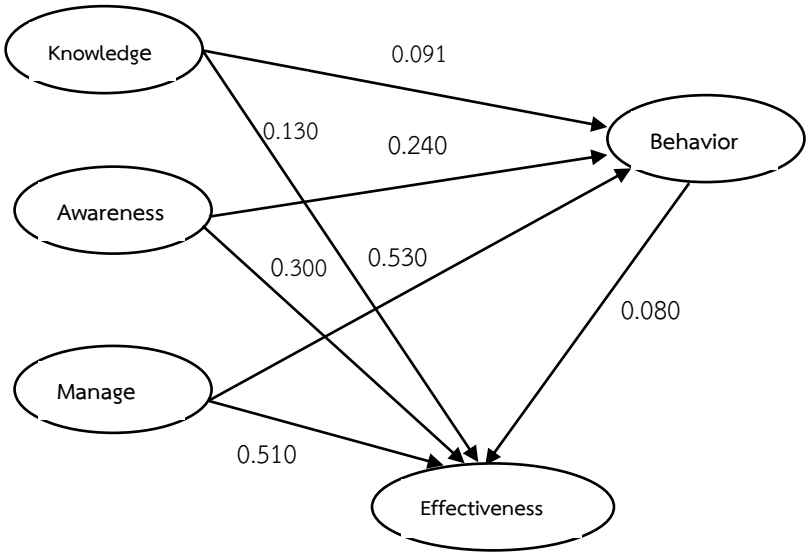
*Correlation is significant at the 0.05 level (2-tailed)



ภาพที่ 3 ตัวแบบปัจจัยเชิงสาเหตุที่มีอิทธิพลต่อประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศ หลังปรับรูปแบบโมเดล

ผลการวิเคราะห์ข้อมูลหลังปรับรูปแบบพบว่า ดัชนีที่ใช้ในการตรวจสอบความสอดคล้องและความกลมกลืนของตัวแปรกับข้อมูลเชิงประจักษ์ของสมการโครงสร้างผ่านเกณฑ์ที่กำหนดที่สามารถยอมรับตัวแบบสมการโครงสร้างได้ สรุปได้ว่าตัวแบบมีความสอดคล้องและความกลมกลืน (model fit)

โดยผลการวิเคราะห์ข้อมูลพบว่า ค่าความสอดคล้องสมการโครงสร้างตามสมมติฐานกับสมการโครงสร้างภายหลังการปรับตัวแบบ มีความสอดคล้องกับข้อมูลเชิงประจักษ์ พิจารณาได้จากค่าดัชนีความสอดคล้องมีค่าตามเกณฑ์ ยกเว้นค่า p-value=0.0001 ซึ่งมีนัยสำคัญทางสถิติที่ 0.05 จึงไม่ผ่านเกณฑ์ ดังนั้นจึงแก้ไขโดยการพิจารณาจากค่าอัตราส่วนของไคสแควร์ต่อองศาความเป็นอิสระ (Chi-square to degree of freedom ratio : Chi-square/df) ซึ่งโดยทั่วไปต้องมีค่าน้อยกว่า 3.00 จะถือว่าแบบจำลองเข้ากันได้ดีกับข้อมูล (Hair et al., 2010) และเมื่อพิจารณาค่าสถิติตามเงื่อนไขพบว่าหลังปรับรูปแบบค่าสถิติที่คำนวณได้ผ่านเกณฑ์ทั้งหมด คือ ค่า Chi-square/df = 2.63, GFI = 0.94, AGFI = 0.90, CFI = 0.98, RMSEA = 0.072 โดยองค์ประกอบของตัวแปรแฝงมีค่าความสัมพันธ์อยู่ระหว่าง 0.21 ถึง 0.83 และมีค่าน้ำหนักองค์ประกอบอยู่ระหว่าง 0.558 ถึง 0.879 ดังนั้นตัวแบบสมการโครงสร้างนี้มีประสิทธิภาพในการวัด มีความสอดคล้องกับข้อมูลเชิงประจักษ์ จึงทำการทดสอบอิทธิพลทั้งทางตรงและทดสอบอิทธิพลทางอ้อมของตัวแปรคั่นกลางพฤติกรรมการใช้งานสารสนเทศ ในแบบจำลองสมการโครงสร้าง ผลจากการทดสอบรายละเอียด ดังภาพที่ 4



ภาพที่ 4 Diagram อิทธิพลทางตรง และอิทธิพลทางอ้อมต่อประสิทธิผลของการจัดการความปลอดภัยของสารสนเทศ

จากภาพที่ 4 พบว่าความรู้ด้านสารสนเทศ การตระหนักรู้สารสนเทศ และการบริหารจัดการสารสนเทศ มีอิทธิพลทางตรงกับพฤติกรรมการใช้สารสนเทศ และพบว่า มีอิทธิพลทางตรงกับประสิทธิผลของการจัดการความปลอดภัยของสารสนเทศ และพบว่า ความรู้ด้านสารสนเทศ การตระหนักรู้สารสนเทศ และการจัดการสารสนเทศ มีอิทธิพลทางอ้อมต่อประสิทธิผลของการจัดการความปลอดภัยของสารสนเทศ ผ่านพฤติกรรมการใช้สารสนเทศ เป็นไปตามสมมติฐานที่ตั้งไว้ทั้ง 5 สมมติฐาน

การวิจัยเชิงคุณภาพ

ผลการสนทนากลุ่ม (Focus Group) ทีมพัฒนาคุณภาพ (Quality Steering Team : QST) ของโรงพยาบาลสระบุรี โดยใช้ข้อคำถามปลายเปิดในการสนทนา ผู้บริหารมีความเห็นตรงกันว่า ถ้าจะให้เกิดประสิทธิผลของการจัดการความปลอดภัยของสารสนเทศ บุคลากรทุกคนต้อง มีพฤติกรรมในการใช้สารสนเทศที่เหมาะสม ต้องปฏิบัติตามนโยบายที่กำหนดไว้ ต้องมีระบบการควบคุมกำกับ และติดตาม มีการกำหนดสิทธิการเข้าถึงข้อมูลที่เหมาะสม และที่สำคัญ เจ้าหน้าที่ต้องมีความรู้ มีความตระหนักรู้ มีการประยุกต์ใช้ความรู้ให้เหมาะสมกับสถานการณ์เพื่อป้องกัน หรือเพื่อรับมือกับภาวะวิกฤตที่อาจจะเกิดขึ้นในอนาคต ซึ่งสนับสนุนกับผลการวิจัยเชิงปริมาณที่พบว่าความรู้ด้านสารสนเทศ การตระหนักรู้สารสนเทศ การบริหารจัดการสารสนเทศ และพฤติกรรมการใช้สารสนเทศ มีอิทธิพลต่อประสิทธิผลของการจัดการความปลอดภัยของสารสนเทศ นอกจากนี้ผู้บริหารยังให้ความสำคัญกับการสร้างแนวทางการปฏิบัติเพื่อความปลอดภัยของระบบและมีการปรับปรุงอย่างต่อเนื่อง โดยรายละเอียดของแนวทางปฏิบัติควรแยกให้ชัดเจนระหว่างผู้ที่ทำหน้าที่ผู้แลระบบและผู้ที่ใช้งาน ซึ่งประกอบด้วย

ส่วนของผู้ดูแลระบบ

1. การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ
2. การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล
3. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
4. การตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

ส่วนของผู้ใช้งาน เน้นเรื่องความรู้ความเข้าใจ ความตระหนักและพฤติกรรมการใช้งานสารสนเทศ

อภิปรายผลการวิจัย

ความรู้ด้านสารสนเทศ ส่งผลต่อประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศโรงพยาบาลสระบุรี

ความรู้ด้านสารสนเทศ แบ่งประเด็นการศึกษาเป็น 3 ประเด็นย่อย คือการประยุกต์ใช้สารสนเทศสนเทศ การประเมินผล และการวิเคราะห์สารสนเทศ เมื่อนำข้อมูลที่รวบรวมจากบุคลากรของโรงพยาบาลสระบุรี และนำมาวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis : EFA) พบว่า ประเด็นในเรื่องการรับรู้สารสนเทศ ที่อยู่ในหมวดของการตระหนักรู้สารสนเทศเข้ามารวมอยู่ในหมวดของความรู้ด้านสารสนเทศ สนับสนุนทฤษฎีของ Bloom (1956) กล่าวไว้ว่า การรับรู้เป็นความรู้หลักปฏิบัติที่ถูกต้อง จึงเป็นไปได้ที่ผลการวิเคราะห์องค์ประกอบเชิงสำรวจประเด็นของการรับรู้จึงเข้ามารวมอยู่ในหมวดของความรู้ด้านสารสนเทศ ผลการทดสอบอิทธิพลของความรู้ด้านสารสนเทศพบว่า ส่งผลต่อประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศ สอดคล้องกับงานวิจัย (อนันต์ ชูยิ่งสกุลทิพย์, 2562) พบว่า ความรู้ส่งผลต่อการพัฒนาด้านสมรรถนะด้านเทคโนโลยีสารสนเทศ และ

งานวิจัย (Hassandoust & Techatassanasoontorn, 2020) พบว่า ความรู้เกี่ยวกับภัยคุกคามส่งผลต่อความปลอดภัยของสารสนเทศ และสนับสนุนงานวิจัย (Ulsamer et al., 2021; Stefaniuk, 2020) พบว่า ความรู้ เป็นสิ่งที่จำเป็นต่อความปลอดภัยของข้อมูล ความรู้มีความสัมพันธ์กับความปลอดภัยของข้อมูล สำหรับในมุมมองของผู้บริหารจากการสนทนากลุ่มเห็นว่าความรู้ด้านความปลอดภัยของสารสนเทศเป็นสิ่งที่สำคัญ ผู้รับผิดชอบต้องส่งเสริมการให้ความรู้ กับบุคลากรอย่างต่อเนื่องและสม่ำเสมอ

การตระหนักรู้สารสนเทศ ส่งผลต่อประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศ โรงพยาบาลสระบุรี

การตระหนักรู้สารสนเทศ แบ่งเป็น 3 ประเด็นย่อยคือ การรับรู้สารสนเทศ ความเข้าใจสารสนเทศ การวิเคราะห์สถานการณ์ เมื่อนำข้อมูลที่รวบรวมจากบุคลากรของโรงพยาบาลสระบุรีและนำมาวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis : EFA) พบว่า ประเด็นในเรื่องการรับรู้สารนเทศ ไปรวมอยู่ในในหมวดของ ความรู้ด้านสารสนเทศ สนับสนุนทฤษฎีการเรียนรู้ ของ Bloom (1956) ระบุไว้ว่า การรับรู้ เป็นความรู้หลักปฏิบัติที่ถูกต้อง ผลการทดสอบอิทธิพลของการตระหนักรู้สารสนเทศพบว่า ส่งผลต่อประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศ สอดคล้องกับงานวิจัย (Thangavelu et al., 2020) พบว่า ความตระหนักมีผลต่อความปลอดภัยของสารสนเทศ และงานวิจัย (Hwang et al., 2021) พบว่า ความตระหนักเป็นสิ่งที่สำคัญต่อความปลอดภัยของระบบสารสนเทศ และงานวิจัย (Karabatak & Karabatak, 2019) พบว่า ความตระหนักของผู้บริหารเป็นสิ่งที่สำคัญต่อการสร้างความปลอดภัยของสารสนเทศ สำหรับในมุมมองของผู้บริหารจากการสนทนากลุ่มเห็นว่าบุคลากรของโรงพยาบาลสระบุรีไม่ค่อยมีความตระหนักในเรื่องของความปลอดภัยระบบสารสนเทศเท่าที่ควร สนับสนุนแนวคิดของผู้เชี่ยวชาญที่ศูนย์ไซเบอร์กองทัพอากาศ ศูนย์ประสานความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ประเทศไทย และคณะกรรมการไซเบอร์แห่งชาติ ที่เน้นให้ผู้ที่มีหน้าที่ดูแลสารสนเทศของโรงพยาบาลสระบุรี กระตุ้นบุคลากรของโรงพยาบาลให้มีความตื่นตัวและตระหนักว่า อาชญากรรมทางไซเบอร์เป็นสิ่งที่ใกล้ตัว และเกิดขึ้นได้ตลอดเวลา ทั้งนี้อาจเนื่องมาจากความกังวลจากผลกระทบของการเกิดภาวะวิกฤติกับฐานข้อมูลของโรงพยาบาลสระบุรีที่ผ่านมา

การบริหารจัดการสารสนเทศส่งผลต่อประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศ โรงพยาบาลสระบุรี

การบริหารจัดการสารสนเทศ แบ่งเป็น 3 ประเด็นย่อยคือ การวางแผน การจัดการ และ การควบคุมกำกับ พบว่า ภาพรวมอยู่ในระดับมาก สนับสนุนทฤษฎี POCCC ของ Fayol 1964) ที่กำหนดไว้ว่าการบริหารจัดการสารสนเทศให้เกิดความมั่นคงปลอดภัย ต้องประกอบด้วย 1) การวางแผน (Plan) 2) การบริหารจัดการ (การบริหารจัดการองค์กร (Organizing) การบังคับบัญชาของหัวหน้างาน (Commanding) การจัดการในเรื่องการประสานงาน (Coordination) และ3) การควบคุมกำกับ (Controlling) สนับสนุนมาตรฐานความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน (Health

Accreditation Information Technology: HAiT) ระบุไว้ว่า มาตรฐานการควบคุมคุณภาพของเทคโนโลยีสารสนเทศต้องมีการวางแนวการจัดการสารสนเทศเพื่อลดความเสี่ยง สร้างความปลอดภัยในระบบเทคโนโลยีสารสนเทศ มีระบบการควบคุมคุณภาพข้อมูล ผลการทดสอบอิทธิพลของการจัดการสารสนเทศพบว่า ส่งผลต่อประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศสอดคล้องกับการวิจัย (นิตยปภา จันทะปัสสา, 2561) พบว่า การพัฒนาสารสนเทศต้องมีการจัดการสารสนเทศตามขั้นตอนการพัฒนาระบบสารสนเทศ โดยใช้กลยุทธ์ในการพัฒนา การบริหารงานบุคคล ทำให้บุคลากรมีความรู้ความเข้าใจและทักษะในการใช้สารสนเทศ สอดคล้องกับงานวิจัย (Arbanas & Žajdela Hrustek, 2019) พบว่า องค์กรจะจัดการรักษาความปลอดภัยให้สำเร็จโดยการสนับสนุนด้านการจัดการ มีนโยบายการรักษาความปลอดภัยของ สำหรับในมุมมองของผู้บริหารจากการสนทนากลุ่มพบว่า ถ้าจะให้ระบบสารสนเทศของโรงพยาบาลสระบุรีมีความปลอดภัยจากการถูกโจมตี ควรต้องมีระบบการจัดการ แยกคอมพิวเตอร์ในการปฏิบัติงานเป็นส่วนของการใช้งานเพื่อรักษาพยาบาลผู้ป่วยกับส่วนของการใช้งานสำหรับสำนักงาน ะมีมาตรการรับมือที่เหมาะสมและหาวิธีจัดการเทคโนโลยีสารสนเทศให้มีความปลอดภัย

พฤติกรรมการใช้งานระบบสารสนเทศส่งผลต่อประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศ โรงพยาบาลสระบุรี

พฤติกรรมการใช้งานสารสนเทศ ในงานวิจัยนี้แบ่งพฤติกรรมการใช้สารสนเทศออกเป็น 3 ประเด็นย่อยคือ ความสามารถในการใช้สารสนเทศ ความต้องการใช้สารสนเทศ และแรงจูงใจในการใช้สารสนเทศ พบว่าภาพรวมอยู่ในระดับมากสนับสนุนทฤษฎีของ Maslow (1954) ที่กล่าวว่า แรงจูงใจ จะเป็นพลังให้เกิดพฤติกรรม สำหรับทฤษฎีของ Bloom (1956) กล่าวถึงพฤติกรรมด้านการปฏิบัติ ว่าเป็นพฤติกรรมที่ใช้ความสามารถทางร่างกาย ผลการทดสอบอิทธิพลของการพฤติกรรมการใช้สารสนเทศพบว่า ส่งผลต่อประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศ เช่นเดียวกับการศึกษาของ Safa et al. (2019) พบว่า พฤติกรรมมีอิทธิพลต่อความปลอดภัยของข้อมูล การเปลี่ยนแปลงพฤติกรรมที่ดี นำไปสู่ความสำเร็จด้านความปลอดภัยทางไซเบอร์ สำหรับในมุมมองของผู้บริหารจากการสนทนากลุ่มพบว่า พฤติกรรมการใช้งานสารสนเทศ ของบุคลากรของโรงพยาบาลสระบุรี ไม่ค่อยเหมาะสมเท่าที่ควร ต้องการความสะดวกในการเข้าใช้งานในระบบสารสนเทศ การใช้งานไม่ค่อยมีความระแวดระวังมากเท่าที่ควร สนับสนุนแนวคิดของ ผู้เชี่ยวชาญจากศูนย์ไซเบอร์กองทัพอากาศ ศูนย์ประสานความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ประเทศไทย และคณะกรรมการไซเบอร์แห่งชาติ ที่เน้นย้ำว่า โรงพยาบาลสระบุรี ต้องหาวิธีการให้บุคลากรมีพฤติกรรมการใช้งานสารสนเทศที่เหมาะสมเพื่อให้สารสนเทศมีความปลอดภัย

ประสิทธิผลของการจัดการความปลอดภัยสารสนเทศ

ประสิทธิผลของการจัดการความปลอดภัยของสารสนเทศ โดยมีประเด็นย่อยที่สำคัญของการศึกษา จากเดิม 3 ประเด็น คือ การรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ของ

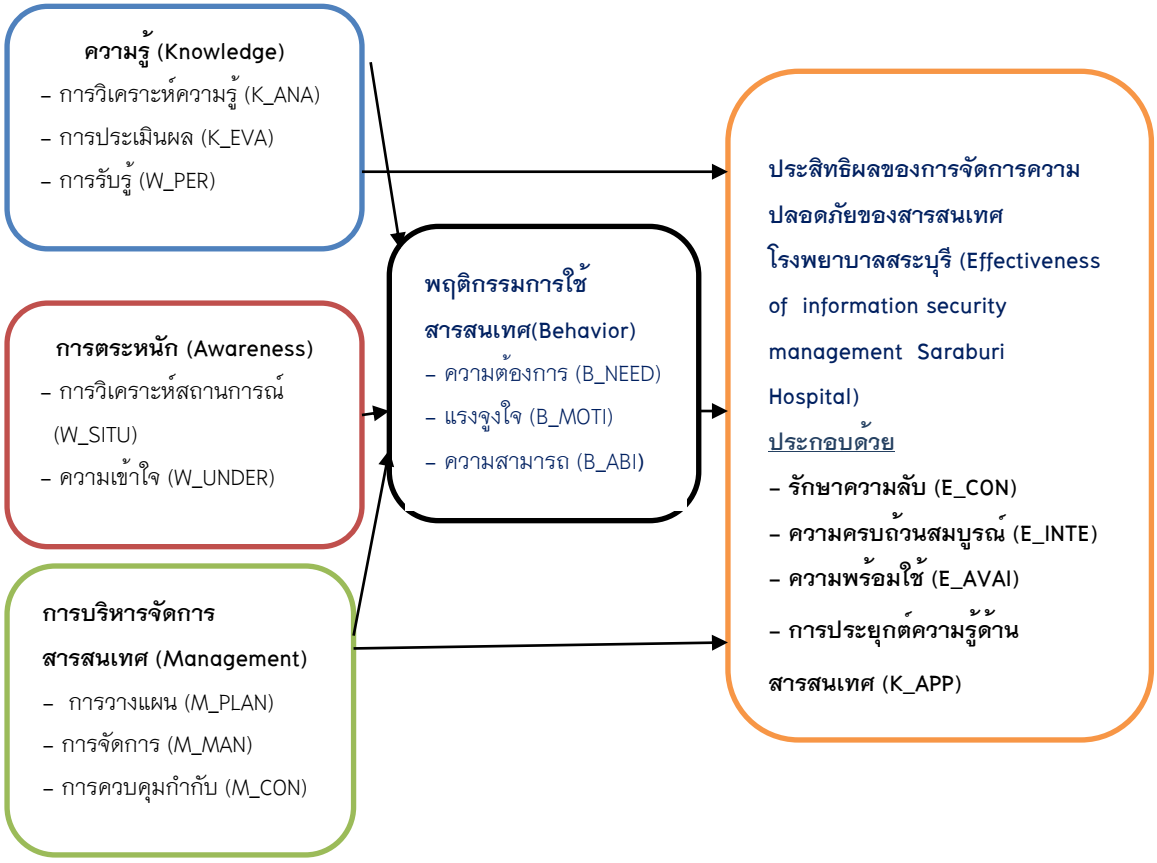
สารสนเทศ (Integrity) และความพร้อมใช้สารสนเทศ (Availability) สนับสนุนแนวคิดด้านความปลอดภัยของระบบสารสนเทศ ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transactions Development Agency :Thai CERT) และการรักษาความปลอดภัยของข้อมูลสารสนเทศตามมาตรฐาน (Health Accreditation Information Technology : HAiT) ที่กำหนดไว้ว่า ปลอดภัยของระบบสารสนเทศมีลักษณะ "C.I.A Triangle" คือมีลักษณะเป็นความลับ (Confidentiality) สารสนเทศต้องมีความสมบูรณ์ (Integrity) และมีความพร้อมใช้งานอยู่ตลอดเวลา(Availability) แต่เมื่อนำข้อมูลที่รวบรวมจากบุคลากรของโรงพยาบาลสระบุรีและนำมาวิเคราะห์ พบว่า ประสิทธิผลของการจัดการความปลอดภัยของสารสนเทศ มีประเด็นย่อยที่น่าสนใจเพิ่มขึ้น คือ เรื่องการประยุกต์ความรู้สารสนเทศ สนับสนุนแนวคิดและมุมมองของผู้บริหารโรงพยาบาลสระบุรี ที่มีความเห็นว่าบุคลากรโรงพยาบาลสระบุรี ต้องรู้จักประยุกต์ใช้ความรู้ทางเทคโนโลยีสารสนเทศ ให้เหมาะสมกับสถานการณ์เพื่อรับมือกับภาวะวิกฤตที่อาจจะเกิดขึ้นในอนาคต โดยผลการทดสอบปัจจัยที่ส่งผลประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศด้วยการวิเคราะห์เส้นทาง (Path Analysis) พบว่า เส้นทางความสัมพันธ์ของ ประสิทธิผลของการจัดการระบบสารสนเทศของโรงพยาบาลสระบุรี ได้รับอิทธิพลทั้งทางตรงและทางอ้อมจาก ความรู้ด้านสารสนเทศ การตระหนักรู้สารสนเทศ การบริหารจัดการสารสนเทศและพฤติกรรมการใช้งานสารสนเทศ และพบว่าการบริหารจัดการสารสนเทศส่งผลทั้งทางตรงและทางอ้อมมากที่สุด

แนวทางในการปฏิบัติงานเพื่อสร้างความปลอดภัยของระบบสารสนเทศ โรงพยาบาลสระบุรี

จากผลของการวิจัยเชิงปริมาณและการสนทนากลุ่ม พบว่าสิ่งที่สำคัญที่ทำให้สารสนเทศมีประสิทธิผลและมีความปลอดภัย นอกเหนือจากความรู้ การตระหนักรู้ และพฤติกรรมการใช้งานสารสนเทศของบุคลากรของโรงพยาบาลสระบุรี สิ่งที่ต้องมีคือการบริหารจัดการ การสร้างแนวทางการปฏิบัติงาน ให้สอดคล้องกับนโยบายและทรัพยากรของโรงพยาบาล สามารถนำไปใช้งานได้จริง สิ่งที่สำคัญในการจัดการสารสนเทศคือ มนุษย์ ซึ่งเป็นทั้งผู้สร้าง ผู้ปฏิบัติงาน และผู้ต้องการใช้สารสนเทศ ทำให้สารสนเทศมีค่าและมีความหมาย การจัดการให้สารสนเทศ มีประสิทธิผล จึงควรมุ่งไปที่แนวทางปฏิบัติ ซึ่งเปรียบเสมือนแผนที่บอกเส้นทางการทำงาน ให้เป็นแนวทางเดียวกัน สอดคล้องกับการศึกษาของ Szczepaniuk et al. (2020) ที่พบว่าการจัดการสารสนเทศ ด้านความปลอดภัยของข้อมูลในการบริหารภาครัฐจำเป็นต้องมีแนวทางและมีการจัดการเชิงระบบ เพื่อให้เกิดการพัฒนาและปรับปรุง นั่นคือบุคลากรต้องมีความเข้าใจวิธีการที่ถูกต้อง โดยแยกให้ชัดเจนระหว่างผู้ที่ทำหน้าที่ผู้แลระบบและผู้ที่ใช้งาน มีการกำกับและติดตามงานได้ทุกขั้นตอน มีการปรับปรุงแนวทางปฏิบัติอย่างต่อเนื่อง จะก่อให้เกิดประโยชน์สำหรับการใช้งาน การป้องกัน และการรับมือกับภัยคุกคามที่อาจเกิดขึ้นทุกช่วงขณะตลอดเวลา ได้อย่างทันต่อเหตุการณ์

องค์ความรู้ใหม่จากการวิจัย

ผลจากการศึกษาประสิทธิผลการจัดการความปลอดภัยระบบสารสนเทศโรงพยาบาลสระบุรี ผู้วิจัยได้สังเคราะห์หลักการ แนวคิด และทฤษฎีที่เกี่ยวข้อง สรุปเป็นองค์ประกอบของการจัดการความปลอดภัยของระบบสารสนเทศขึ้น เรียกว่า "C.I.A Triangle" ประกอบด้วยความลับ (Confidentiality: C) ความสมบูรณ์ (Integrity :I) และความพร้อมใช้งาน(Availability :A) แต่จากผลของการวิจัยทั้งในส่วนของการวิจัยเชิงปริมาณ และการสนทนากลุ่มผู้บริหารคุณภาพ พบว่าประเด็นที่สำคัญที่เป็นองค์ประกอบของการจัดการความปลอดภัยของสารสนเทศ นอกเหนือจาก C.I.A Triangle คือการประยุกต์ความรู้สารสนเทศ ผู้วิจัยจึงนำมากำหนดองค์ประกอบของการจัดการความปลอดภัยของสารสนเทศโรงพยาบาลสระบุรีเป็นองค์ความรู้ใหม่ของประสิทธิผลการจัดการความปลอดภัยของสารสนเทศโรงพยาบาลสระบุรี ดังภาพที่ 4



ภาพที่ 4 องค์ประกอบของประสิทธิผลการจัดการความปลอดภัยของระบบสารสนเทศ โรงพยาบาลสระบุรี

สรุป

ผลของการศึกษานอกจากจะทำให้ทราบถึงเส้นทางของปัจจัยที่มีอิทธิพลต่อการจัดการความปลอดภัยของระบบสารสนเทศของโรงพยาบาลสระบุรี ซึ่งประกอบด้วยความพร้อมใช้ (availability) ความครบถ้วนสมบูรณ์ (Integrity) การรักษาความลับ(Confidentiality)และประยุกต์ความรู้สารสนเทศ

(Knowledge apply) โดยปัจจัยที่มีอิทธิพลมากที่สุดคือในเรื่องของการบริหารจัดการสารสนเทศ รองมาเป็นเรื่องของ การตระหนักรู้สารสนเทศ ความรู้และพฤติกรรมในการใช้งานสารสนเทศ สนับสนุนแนวคิดของผู้เชี่ยวชาญจาก ศูนย์ไซเบอร์กองทัพอากาศ ศูนย์ประสานความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ประเทศไทย และคณะกรรมการไซเบอร์แห่งชาติ ที่เสนอให้โรงพยาบาลสระบุรี ออกนโยบายขององค์กรมุ่งเน้นให้มีการรับรู้และความตระหนักในด้านความปลอดภัย มุ่งส่งเสริมการให้ความรู้ กระตุ้นให้มีความตื่นตัวและตระหนักว่า อาชญากรรมทางไซเบอร์ เป็นสิ่งที่ใกล้ตัวและเกิดขึ้นได้ บุคลากรต้องมีพฤติกรรมการใช้งานที่เหมาะสม สอดคล้องกับแนวคิดของผู้บริหารจากการสนทนากลุ่มที่มีความเห็นว่า บุคลากรของโรงพยาบาลสระบุรี ต้องมีความรู้ มีความตระหนัก รู้จักประยุกต์ใช้ความรู้ให้เหมาะสมกับสถานการณ์ ที่อาจจะเกิดขึ้นในอนาคต ที่สำคัญควรมีการสร้างแนวทางการปฏิบัติและควรมีการปรับปรุงอย่างต่อเนื่อง โดยแนวทางการปฏิบัติงานควรแบ่งเป็นในส่วนของผู้ดูแลระบบและส่วนของผู้ใช้งานสารสนเทศ จึงจะเกิดประโยชน์สำหรับการใช้งาน การป้องกันและการรับมือกับภัยคุกคาม ได้อย่างทันต่อเหตุการณ์

ข้อเสนอแนะ

ข้อเสนอแนะในการนำผลวิจัยไปใช้ประโยชน์

ความมั่นคงปลอดภัยไม่ได้เกิดขึ้นที่ซอฟต์แวร์ และฮาร์ดแวร์เพียงอย่างเดียว แต่การรักษาความมั่นคงปลอดภัยของสารสนเทศเป็นกระบวนการ (Process) ต้องอาศัยความร่วมมือจากผู้ใช้งานทั้งผู้ดูแลระบบและผู้ใช้งานทั่วไป ต้องกำหนดนโยบายและมาตรการที่ทำให้เกิดการปฏิบัติที่มุ่งไปสู่เป้าหมายเดียวกัน มีวิธีการจัดการเทคโนโลยีให้มีความปลอดภัย มีระบบการป้องกันและมาตรการรับมือที่เหมาะสมมีระบบการควบคุมกำกับติดตาม และมีบทลงโทษหากไม่ปฏิบัติตามนโยบายที่กำหนดไว้ ในส่วนของการสำรองข้อมูลที่ทำอยู่ในปัจจุบันยังไม่ปลอดภัย และมีจำนวนที่ไม่เพียงพอ ต้องหาวิธีการจัดการให้เหมาะสมและมีความปลอดภัย ถ้าเกิดภาวะวิกฤตต้องสามารถนำกลับกลับมากู้คืนระบบได้ในเวลาอันรวดเร็ว ลดผลกระทบจากการสูญเสียรายได้ และ การให้บริการประชาชน

ข้อเสนอแนะในการวิจัยครั้งต่อไป

การวิจัยครั้งต่อไปควรศึกษาเพิ่มเติมในเรื่องการแบ่งกลุ่มประชากรที่ศึกษา เป็นกลุ่มผู้ที่ทำหน้าที่ ควบคุมดูแลระบบเทคโนโลยีสารสเทศ และกลุ่มผู้ใช้สารสารสนเทศ เพื่อนำผลที่ได้ไปแก้ปัญหาในแต่ละกลุ่ม และนำผลการศึกษาที่ได้รับไปใช้ในการพัฒนาศักยภาพให้ชัดเจน เหมาะสมและตรงตามกลุ่มเป้าหมายเพื่อสร้างระบบสารสนเทศให้มีความปลอดภัย

เอกสารอ้างอิง

ชุษณะ มกรสาร และ วรรษา เปาอินทร์. (2561). *Thai Medical Informatics–TMI Hospital IT Maturity Model. แนวทางการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาล*. นนทบุรี: กระทรวงสาธารณสุข.

นิตยปภา จันทะปัสสา. (2562). การพัฒนาระบบสารสนเทศการบริหารงานบุคคล โรงเรียนบ้านดอนตูม ดอนโด สำนักงานเขตพื้นที่การศึกษาประถมศึกษา มหาสารคาม เขต 1. *วารสารวิชาการและวิจัย มหาวิทยาลัยภาคตะวันออกเฉียงเหนือ, 9*(1), 82–89.

นิพิฐพนธ์ สนิทเหลือ, วัชรีพร สาตร์เพ็ชร์ และ ญาดา นภาอารักษ์. (2562). การคำนวณขนาดตัวอย่างด้วย โปรแกรมสำเร็จรูป G* Power. *วารสารสถาบันเทคโนโลยีแห่งสุวรรณภูมิ, 5*(1), 496–507.

ภิรมย์ กมลรัตนกุล. (2550). *หลักการทำวิจัยให้สำเร็จ.* (พิมพ์ครั้งที่ 5). กรุงเทพฯ: เท็กซ์ แอนด์ เจอร์นัลพับลิเคชั่น.

โรงพยาบาลสระบุรี. (2565). *ฐานข้อมูลการเงิน.* สืบค้นเมื่อ 14 กุมภาพันธ์ 2565, จาก http://Intranet.srbr.in.th/Finance/

วศินี หนุนภักดี. (2562). การวิเคราะห์ความเสี่ยงของผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของหน่วยงานภาครัฐในยุคเศรษฐกิจดิจิทัล. *วารสารบัณฑิตวิทยาลัย มหาวิทยาลัยสวนดุสิต, 13*(2),173–187.

สมศิริ พันธุ์ศักดิ์ศิริ และ เสาวนีย์ สมันตรีพร. (2565). ภาวะวิกฤติของระบบสารสนเทศโรงพยาบาลสระบุรี. *วารสารนวัตกรรมการจัดการศึกษาและวิจัย, 5*(1), 127–136.

สมศิริ พันธุ์ศักดิ์ศิริ. (2562). การพัฒนาระบบบันทึกข้อมูลการเคลื่อนย้ายผู้ป่วยออนไลน์ โรงพยาบาลสระบุรี. *วารสารโรงพยาบาลแพร่, 27*(2), 93–109.

อดิศักดิ์ ถีระแก้ว และ ปุญชรัศมิ์ ศักดิ์ธรรมเจริญ. (2561). ประสิทธิผลและความพึงพอใจของการให้ความรู้แก่ผู้ป่วยต่อการใช้เอกสารอิเล็กทรอนิกส์ ร่วมกับเอกสารคำแนะนำสำหรับผู้ป่วยมะเร็งที่รับการรักษาด้วยรังสี. *Journal of Thai Association of Radiation Oncology, 24*(1), 14–24.

อนันต์ ชูยิ่งสกุลทิพย์. (2562). ระบบพัฒนาสมรรถนะด้านเทคโนโลยีสารสนเทศ และการสื่อสารเพื่อความมั่นคงปลอดภัยของสารสนเทศ. *วารสารสนเทศศาสตร์, 37*(3), 59–80.

อานนท์ ไทยเจริญ และ สมศิริ พันธุ์ศักดิ์ศิริ. (2564). ระบบสารสนเทศโรงพยาบาลสระบุรี: ประสบการณ์และโอกาสพัฒนา. *วารสารโรงพยาบาลสระบุรี, 26*(70), 43–52.

Arbanas, K., & Žajdela Hrustek, N. (2019). Key Success Factors of Information Systems Security. *Journal of Information and Organizational Sciences, 43*(2), 131–144.

Bloom, B. S. (1956). *Taxonomy of educational objectives. Vol. 1: Cognitive Domain*. New York: McKay.

Chesti, I. A., Humayun, M., Sama, N. U., & Jhanjhi, N. Z. (2020, October). Evolution, mitigation, and prevention of ransomware. In *2020 2nd International Conference on Computer and Information Sciences (ICCIS)* (pp. 1–6). IEEE.

Cohen, J. (1992). Statistical Power Analysis. *Current Directions in Psychological Science, 1*(3), 98–101.

Edwards, J. S. (2022). Where Knowledge Management and Information Management Meet: Research Directions. *International Journal of Information Management, 63*, 102458.

Fayol, H. (2016). *General and Industrial Management.* Ravenio Books.

Gross, B. M. (1972). *Mathematical models in linguistics*. New Jersey: Prentice–Hall

Hair, J. F., Black, W.C, Babin, B.J., & Anderson, R. E (2010). *Multivariate Data Analysis*. (7th ed.). New Jersey: Pearson Education.

Hassandoust, F., & Techatassanasoontorn, A. A. (2020). Understanding Users' Information Security Awareness and Intentions: A Full Nomology of Protection Motivation Theory. In *Cyber Influence and Cognitive Threats.* (pp. 129–143). Academic Press.

Hong, S., Park, S., Park, L. W., Jeon, M., & Chang, H. (2018). An Analysis of Security Systems for Electronic Information for Establishing Secure Internet of Things Environments: Focusing on Research Trends in The Security Field in South Korea. *Future Generation Computer Systems, 82*, 769–782.

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2021). Security Awareness: The First Step in Information Security Compliance Behavior. *Journal of Computer Information Systems, 61*(4), 345–356.

Karabatak, S., & Karabatak, M. (2019). Information security awareness of school administrators. In *2019 7th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1–6). IEEE.

Maslow, A. H. (1954). Motivation and Personality. New York: Harper and Row.

Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., & Sookhak, M. (2019). Deterrence And Prevention–Based Model to Mitigate Information Security Insider Threats in Organizations. *Future Generation Computer Systems, 97*, 587–597.

Schermerhorn, J. R., Hunt, J. G., & Osborn, R. N. (1991). *Managing Organizational Behavior*. New York: Wiley.

Stefaniuk, T. (2020). Training in Shaping Employee Information Security Awareness. *Entrepreneurship and Sustainability Issues, 7*(3), 1832.

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information Security Assessment in Public Administration. *Computers & Security, 90*, 101709.

Thangavelu, M., Krishnaswamy, V., & Sharma, M. (2020). Comprehensive Information Security Awareness (CISA) in Security Incident Management (SIM): A Conceptualization. *South Asian Journal of Management, 27*(2), 160–188.