ภาวะวิกฤติของระบบสารสนเทศโรงพยาบาลสระบุรี

The crisis of information system in Saraburi Hospital

[1]สมศิริ พันธุ์ศักดิ์ศิริ และ [2]เสาวนีย์ สมันต์ตรีพร

Somsiri Pansaksiri and Saowanee Samantreeporn

บัณฑิตวิทยาลัย มหาวิทยาลัยเอเชียอาคเนย์

Graduate School, Southeast Asia University, Thailand.

[1]siri.pansaksiri@gmail.com, [2]film.phd5@gmail.com

[2]corresponding author

Received September 28, 2022; **Revised** November 6, 2022; **Accepted** January 7, 2023

บทคัดย่อ

บทความนี้มีวัตถุประสงค์ 1) เพื่อศึกษาสถานการณ์การเกิดภาวะวิกฤตจากการถูกโจมตี ฐานข้อมูลโรงพยาบาลสระบุรี 2) เพื่อหาสาเหตุที่นำไปสู่ความเสี่ยงที่ทำให้เกิด Ransomware Attack การวิจัยเป็นวิจัยเชิงคุณภาพ ศึกษาที่โรงพยาบาลสระบุรี ผู้ให้ข้อมูลสำคัญ เป็นผู้ที่มีส่วนเกี่ยวข้องกับการจัดการและบริหารความเสี่ยงและความปลอดภัยของสารสนเทศโรงพยาบาลสระบุรี จำนวน 9 คน โดยเลือกแบบเฉพาะเจาะจง เครื่องมือที่ใช้ในการวิจัยเป็นแบบสัมภาษณ์กึ่งโครงสร้างวิเคราะห์ข้อมูลโดย ใช้วิเคราะห์เนื้อหา ผลการวิจัยพบว่า

1. สถานการณ์การเกิดภาวะวิกฤตของระบบสารสนเทศ เมื่อถูกไวรัส Ransomware โจมตีด้วยการเข้ารหัสแล้วทิ้ง Email ให้ติดต่อกลับเพื่อเจรจาจำนวนเงินค่าไถ่ ทำให้ฐานข้อมูลที่มีอยู่ไม่สามารถเข้าใช้งานได้ เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศโรงพยาบาลสระบุรีที่มีอยู่ไม่มีความชำนาญและความเชี่ยวชาญ ต้องขอความช่วยเหลือไปยังผู้เชี่ยวชาญที่ ศูนย์ไซเบอร์กองทัพอากาศ กระทรวงดิจิทัลฯ ศูนย์ประสานความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ประเทศไทย คณะกรรมการไซเบอร์แห่งชาติ เพื่อช่วยคลี่คลายสถานการณ์จนกระทั่งสถานการณ์กลับมาเป็นปกติ

2. ภาวะวิกฤติของระบบสารสนเทศโรงพยาบาลสระบุรี สาเหตุที่สำคัญที่พบมาจาก บุคลากรขาดความรู้ความเข้าใจความปลอดภัยของระบบสารสนเทศ ขาดการตระหนักด้านความปลอดภัยของสารสนเทศ วิธีการจัดการให้ฐานข้อมูลยังไม่มีความปลอดภัยทั้งในส่วนของการสำรองข้อมูล การจัดเก็บ และที่สำคัญคือพฤติกรรมที่ไม่เหมาะสมในการใช้สารสนเทศ ต้องมีระบบการจัดการสารสนเทศที่มีประสิทธิภาพ เกิดประสิทธิผลให้กับสารสนเทศของโรงพยาบาลสระบุรีเพื่อให้ระบบมีความมั่นคงและยั่งยืน

คำสำคัญ: ภาวะวิกฤติ; ระบบสารสนเทศ; โรงพยาบาลสระบุรี; Ransomware

Abstract

This article aimed to study the situation of crisis from attack. Information system Saraburi Hospital and to find the factors to the risk of Ransomware Attack. The research model was qualitative. Education at Saraburi Hospital key informant There are 9 people involved in risk management and information security at Saraburi hospital, the sample was purposive sampling,

the instrument for collecting data was Semi-Structure interview. Analysis data by Descriptive statistics and Content Analysis. The research results were found as follows;

1. It was attacked by ransomware which encrypted all databases and files, demanding ransom via email. Saraburi IT personnel didn't have proficiency in handling such emergency, so urgent request for help was sent to Royal Thai Air Force Cyber Center, Ministry of Digital Economy and Society, Thai CERT and National Cyber Security Agency.

2. Saraburi Hospital has learned several important lessons. It is deemed necessary to enhance the knowledge of information security for administrators and user personnel to raise awareness of security and use of information, to improve the management method to make the database of data backup as well as storage, and more importantly to create guidelines for personnel of all work units to have appropriate behavior in using information. There is an efficient information management system for the effectiveness of the information of Saraburi Hospital in order to ensure the stability and sustainability of the system.

Keywords: Crisis; Information system; Saraburi Hospital; Ransomware

บทนำ

ความก้าวหน้าเทคโนโลยีสารสนเทศและการสื่อสาร เป็นพลังขับเคลื่อนสังคมที่นำไปสู่กระบวนทัศน์หรือ Paradigm Shift ในภาคเศรษฐกิจ ธุรกิจ อันส่งผลให้เกิดการเปลี่ยนแปลงทางสิ่งแวดล้อม ประชากร เศรษฐกิจ สังคม และวัฒนธรรม (วศินี หนุนภักดี และคณะ, 2562) เทคโนโลยีสารสนเทศและการสื่อสาร มีคุณประโยชน์หลากหลายประการและเป็นปัจจัยหลักในการพัฒนาประเทศ ช่วยสนับสนุนให้เกิดการพัฒนาทั้งด้านสังคม เศรษฐกิจ อุตสาหกรรม และการพัฒนาคุณภาพชีวิต การเผยแพร่ข้อมูลข่าวสาร การประชาสัมพันธ์และการติดต่อสื่อสารโทรคมนาคม ในลักษณะ เศรษฐศาสตร์ เครือข่าย (networked economy) มีการเปลี่ยนแปลงเคลื่อนย้ายอย่างรวดเร็ว (Hyosung et al., 2018; ศิวลีย์ สิริโรจน์บริรักษ์, 2559) ปรับเปลี่ยนโครงสร้างความสัมพันธ์ ทาง เศรษฐกิจ การเมือง สังคม ระหว่างประเทศ การพัฒนาเทคโนโลยีสื่อสารและสารสนเทศ ส่งผลให้โลกมีสภาพ เหมือนเป็นหนึ่งเดียว เกิดการแข่งขันในวงกว้าง แนวโน้มการพัฒนาเป็นไปทั้งทางด้านบวกและด้านลบ การพัฒนาทางด้านบวก เป็นการพัฒนาเครือข่ายคอมพิวเตอร์ และเครือข่ายอินเทอร์เน็ตที่เชื่อมโยงกันทั่วโลก ก่อให้เกิดการเปลี่ยนแปลงทางสังคม ช่องทางการดำเนินธุรกิจ เช่น การทำธุรกรรมอิเล็กทรอนิกส์ การพาณิชย์อิเล็กทรอนิกส์ การพัฒนาระบบสารสนเทศ ฐานข้อมูล ฐานความรู้ เพื่อการจัดการความรู้ การศึกษาตามอัธยาศัยด้วยระบบอิเล็กทรอนิกส์ (e-learning) การเรียนการสอนด้วยระบบโทรศึกษา

การค้นคว้าหาความรู้ได้ตลอด 24 ชั่วโมง ส่วนแนวโน้มทางด้านลบ คือความผิดพลาดในการทำงานของระบบคอมพิวเตอร์ ทั้งส่วนฮาร์ดแวร์และซอฟต์แวร์ ที่เกิดขึ้นจากการออกแบบและพัฒนา ทำให้เกิดความเสียหายต่อระบบและสูญเสียค่าใช้จ่ายในการแก้ปัญหา การละเมิดลิขสิทธิ์ของทรัพย์สินทางปัญญา การทำสำเนาและลอกเลียนแบบ การก่ออาชญากรรมทางคอมพิวเตอร์ การโจรกรรมข้อมูล การเข้ารหัสข้อมูล การล่วงละเมิด และการก่อกวนระบบ สิ่งเหล่านี้ย่อมส่งผลเสียต่อผู้ใช้งานเมื่อผู้ใช้งานขาดความรู้ในการป้องกันตนเองอย่างเหมาะสม อาจเป็นเหตุนำมาซึ่งความเสื่อมเสียต่อตนเองทั้งข้อมูลและทรัพย์สิน เช่น การถูกหลอกลวงโดยมิจฉาชีพออนไลน์ การขโมยข้อมูลส่วนตัว (อนันต์ ชูยิ่งสกุลวิทย์,2562) องค์กรในระบบการให้บริการด้านสุขภาพหลายแห่งทั้งภาครัฐและเอกชนในประเทศไทยได้มีความพยายามที่จะเปลี่ยนระบบการจัดเก็บข้อมูล จากการใช้ระบบการบันทึกบน

กระดาษมาเป็นระบบเอกสารอิเล็กทรอนิกส์เพื่อลดปัญหาด้านการสื่อสาร การจัดเก็บ การสูญหายของเอกสาร ง่ายต่อการสืบค้นข้อมูลเอกสาร และลดการสิ้นเปลืองทรัพยากรกระดาษ การปรับตัวเพื่อที่จะยอมรับและเรียนรู้เทคโนโลยีใหม่ๆที่เกิดขึ้นโดยเฉพาะระบบข้อมูลและการบริหารจัดการข้อมูลที่ดี จะสามารถสร้างความได้เปรียบและนำไปสู่ความสำเร็จในอนาคตได้ (อดิศักดิ์ ถีระแก้ว และคณะ, 2561) คณะรัฐมนตรีมีมติอนุมัติร่างพระราชบัญญัติว่าด้วยรัฐบาลดิจิทัล เมื่อวันที่ 2 ตุลาคม 2561 กำหนดให้หน่วยงานของรัฐต้องจัดทำข้อมูลตามภารกิจหลักให้อยู่ในรูปแบบข้อมูลดิจิทัล และต้องปรับปรุงข้อมูลดิจิทัลนั้นให้มีความน่าเชื่อถือ มีความถูกต้องทันสมัยสามารถเชื่อมโยงกับหน่วยงานอื่นของรัฐ ผ่านระบบเครือข่ายสารสนเทศและการสื่อสาร และนำไปประมวลผลต่อได้ ด้วยนโยบายจากบริการต่างๆ ดังกล่าวข้างต้น กระทรวงสาธารณสุขจึงเตรียมความพร้อมในด้านโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัล เพื่ออำนวยความสะดวกให้ประชาชน สามารถเข้าถึงการบริการได้อย่างรวดเร็วและข้อมูลของประชาชนมีความมั่นคงปลอดภัย (จิรพล สังข์โพธิ์, 2560)

โรงพยาบาลสระบุรี ได้พัฒนาให้เป็นสถานบริการด้านสุขภาพระดับตติยภูมิระดับสูง เป็นศูนย์เชี่ยวชาญเฉพาะด้าน (Excellent Center) ในเขตภาคกลางตอนบน 5 สาขา ได้แก่ สาขาอุบัติเหตุ การดูแลรักษาผู้ป่วยอุบัติเหตุด้านศัลยกรรมประสาทและศัลยกรรมตกแต่ง, สาขาโรคมะเร็ง, สาขาโรคหัวใจและหลอดเลือด, สาขาทารกแรกเกิด และเป็นศูนย์ความเชี่ยวชาญระดับสูงด้านปลูกถ่ายอวัยวะ ให้บริการตรวจรักษาครอบคลุมประชากร 8 จังหวัด (นนทบุรี, ปทุมธานี, พระนครศรีอยุธยา, สระบุรี, ลพบุรี, สิงห์บุรี, อ่างทอง และนครนายก) โรงพยาบาลสระบุรีได้มีการพัฒนาเทคโนโลยีสารสนเทศมาอย่างต่อเนื่องเพื่อรองรับการให้บริการผู้ป่วยของโรงพยาบาลสระบุรีโดยเฉลี่ยวันละ 2,500 คน โดยพัฒนาระบบเวชระเบียนผู้ป่วยจากการบันทึกในกระดาษเป็นการบันทึกในรูปอิเลคทรอนิกส์ มีระบบฐานข้อมูลการรักษาพยาบาลที่ดี มีคุณภาพ น่าเชื่อถือ สามารถเรียกดูหรือประมวลผลข้อมูลเพื่อนำมาใช้ในการวางแผนการปฏิบัติงานได้ แบบอัตโนมัติ (real time) (สมศิริ พันธุ์ศักดิ์ศิริ, 2562) สำหรับด้านคุณภาพของเทคโนโลยีสารสนเทศได้กำหนดแนวทางการปฏิบัติงานให้มีมาตรฐานของการป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามมาตรฐานของ Healthcare Accreditation Information Technology: HAiT (ชุษณะ มกรสาร และ วรรษา เปาอินทร์,2561) ภาวะวิกฤตเกิดขึ้นเมื่อโรงพยาบาลสระบุรีถูกจารกรรมระบบคอมพิวเตอร์ ด้วยการส่งไวรัสเข้ารหัสข้อมูลเพื่อเรียกค่าไถ่ หรือ Ransomware เข้าสู่ระบบคอมพิวเตอร์ ทำให้โรงพยาบาลเกิดภาวะวิกฤตอย่างมาก ส่งผลให้ฐานข้อมูลผู้ป่วย ระบบเครือข่าย และ ระบบโทรศัพท์ ไม่สามารถใช้งานได้ ความรุนแรงนี้ Chesti, IA, et al, 2020 กล่าวไว้ว่า แรนซัมแวร์หรือมัลแวร์เรียกค่าไถ่เป็นมัลแวร์ ที่ไม่ให้ผู้ใช้งานเข้าถึงไฟล์หรือระบบของตน และต้องการเงินค่าไถ่ ไฟล์ที่ถูกโจมตีจะถูกเข้ารหัสและให้ชำระเงินเป็นดิจิทัลเพื่อถอดรหัสแล้วจึงส่งไฟล์กลับไปยังผู้ใช้อีกครั้ง แรนซัมแวร์ ประเภทนี้เป็นอันตรายเนื่องจากโจมตีไฟล์ทั้งหมดและยากที่จะหาวิธีป้องกัน แม้ว่าการชำระเงินจะเสร็จสิ้น แต่ก็ยังไม่สามารถเป็นหลักประกันได้ว่าไฟล์ จะถูกส่งกลับไปยังเจ้าของข้อมูล ในช่วงสามปีที่ผ่านมา แรนซัมแวร์ได้กลายเป็นหนึ่งในกลโกงทางไซเบอร์ที่ใหญ่ที่สุดที่โจมตีธุรกิจ ประมาณการว่าความสูญเสียที่เกิดขึ้นในปี 2559 เนื่องจากแรนซัมแวร์สูงถึง 1 พันล้านดอลลาร์ โดยมีรูปแบบคือการเข้ารหัสข้อมูลสำคัญบนคอมพิวเตอร์ (Brewer, 2017) การก่อการร้ายทางไซเบอร์กลายเป็นภัยคุกคามสำคัญต่อสันติภาพของโลกและความมั่งคั่งทางเศรษฐกิจของโลก

ความสูญเสียที่เกิดขึ้น ส่งผลให้โรงพยาบาลสระบุรี นอกจากจะประสบปัญหาทางด้านการเข้าถึงข้อมูลผู้ป่วย และระบบเครือข่ายแล้วแล้ว ความสูญเสียด้านการเงินของโรงพยาบาลสระบุรีในช่วงเวลาที่เกิดวิกฤตเทียบกับช่วงเวลาเดียวกันของปีก่อนเกิดภาวะวิกฤติ และปีถัดมาหลังเกิดภาวะวิกฤต พบว่าโรงพยาบาลสระบุรีสูญเสียรายได้ที่เก็บจากการให้บริการตรวจรักษาจากผู้ป่วยนอกและผู้ป่วยในลดลงอย่างมาก จากในช่วงเดือนกันยายนของปี 2562 ถึงปี 2564 การรับรู้รายได้จากการให้บริการตรวจรักษาพยาบาลทั้งผู้ป่วยนอกและผู้ป่วยที่รับไว้รักษาในโรงพยาบาล ในปี 2562 เป็นจำนวนเงิน 100,609,331 บาท สำหรับปี 2563 (เกิดภาวะวิกฤต) รับรู้รายได้ลดลง

เหลือ 32,226,711 บาท และในปี 2564 รับรู้รายได้เป็นจำนวนเงิน 171,721,044 บาท ทำให้รายได้จากการเรียกเก็บเงินจากกองทุน เพื่อนำมาใช้ในการบริหารจัดการ การจัดหาวัสดุอุปกรณ์ การให้บริการและการดูแลรักษาผู้ป่วยลดลง จึงเป็นสิ่งจำเป็นอย่างยิ่งที่ต้องศึกษาสถานการณ์ และสาเหตุของการเกิดภาวะวิกฤติ เพื่อหาวิธีการสร้างความมั่นใจในอนาคตว่า ระบบสารสนเทศของโรงพยาบาลสระบุรีต้องมีความมั่นคง ปลอดภัย ปฏิบัติงานเป็นไปอย่างต่อเนื่องและมีประสิทธิภาพ

วัตถุประสงค์การวิจัย

1. เพื่อศึกษาสถานการณ์การถูกโจมตี ระบบสารสนเทศ โรงพยาบาลสระบุรี
2. เพื่อวิเคราะห์ภาวะวิกฤติของระบบสารสนเทศโรงพยาบาลสระบุรี

การทบทวนวรรณกรรม

การนำเทคโนโลยีเข้ามาใช้เพื่อการรักษาความปลอดภัย เป็นส่วนที่ทำหน้าที่จัดการข้อมูล การประมวลผลและทำ ให้เกิดผลผลิตของระบบออกมาในสื่อที่ต้องการองค์ประกอบที่สำคัญของเทคโนโลยี ได้แก่ คอมพิวเตอร์ ซอฟแวร์ และโทรคมนาคม สำหรับ ฐานข้อมูล (Database) เป็นวิธีการที่จะเก็บข้อมูลอย่างเป็นระบบให้สะดวกต่อการเรียกใช้สามารถแก้ไขได้ง่ายและช่วยสนับสนุนการตัดสินใจของผู้บริหาร เอื้ออำนวยให้ผู้บริหารมีข้อมูลในการประกอบการตัดสินใจได้ดีขึ้น สารสนเทศที่มีการจัดการที่มีประสิทธิผล(Effectiveness) จะช่วยสนับสนุนการตัดสินใจ (Decision Support Systems) สำหรับผู้บริหาร อันจะส่งผลให้การดำเนินการสามารถบรรลุวัตถุประสงค์ที่ตั้งไว้ ระบบที่ดีต้องมีการควบคุม (Control) เพื่อให้ระบบสารสนเทศมีความปลอดภัย ไม่ถูกทำลายทั้งที่เจตนาและไม่เจตนา (Nader Sohrabi Safa , 2019; จิตตกานต์ บุญศิริทิวัตถ์; โกวิท รพีพิศาล,2560) การเกิดความตระหนักที่มุ่งเน้นต่อสถานการณ์ที่จะส่งเสริมการเปลี่ยนแปลง เกี่ยวกับความปลอดภัยของสารสนเทศคือการสร้างความรู้ ความเข้าใจด้านการรักษาความปลอดภัย เพื่อให้มีพฤติกรรมที่สามารถดูแลรักษาและใช้งานทรัพยากรสารสนเทศขององค์กรได้อย่างปลอดภัย (Bloom, ,1956; Choo, & de Alvarenga Neto, 2010) พฤติกรรมจะเกิดขึ้นได้ บุคคลนั้นต้อง มีความรู้(Knowledge) ความสามารถความตระหนักเป็นสิ่งที่สำคัญที่จะนำไปสู่การแสดงออกเป็นพฤติกรรม โดยพฤติกรรมที่จะสร้างความปลอดภัยให้กับระบบสารสนเทศ (Bloom,1956; พลากร ลาภอลงกรณ์, 2565)

ระเบียบวิธีวิจัย

งานวิจัยนี้เป็นงานวิจัยเชิงคุณภาพ ศึกษาที่โรงพยาบาลสระบุรี เลือกกลุ่มตัวอย่างแบบเฉพาะเจาะจง (Purposive Sampling) โดยเลือกเฉพาะ ผู้ที่มีส่วนเกี่ยวข้องกับการบริหารจัดการและดูแลระบบสารสนเทศโดยตรง ประกอบด้วย ประธานคณะกรรมการบริหารความเสี่ยงเของโรงพยาบาลสระบุรี เลขาคณะกรรมการบริหารความเสี่ยงฯ ประธานคณะกรรมการสารสนเทศและเวชระเบียน เลขาคณะกรรมการสารสนเทศและเวชระเบียน ตัวแทนคณะกรรมกรรมสารสนเทศและเวชระเบียน จำนวน 2 คน ผู้ช่วยผู้อำนวยการด้านเทคโนโลยีสารสนเทศ หัวหน้าศูนย์เทคโนโลยีสารสนเทศ และ เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศที่ขึ้นปฏิบัติงานในวันที่เกิดเหตุการณ์ รวมทั้งหมด 9 คน เป็นผู้ให้ข้อมูลคนสำคัญ เก็บรวบรวมข้อมูลโดยใช้แบบสัมภาษณ์กึ่งโครงสร้าง (Semi-structured Interview) มีเนื้อหาประกอบด้วย สถานการณ์ขณะเกิดภาวะวิกฤต ความคิดเห็นถึงสาเหตุและความเสี่ยงที่คาดว่าจะนำไปสู่การเกิดภาวะวิกฤตของระบบสารสนเทศ โดยประเด็นข้อคำถามได้ผ่าน

การตรวจสอบความสอดคล้องของรายละเอียดและวัตถุประสงค์ที่ศึกษา แล้วจำนวน 3 ท่าน ช่วงเวลาที่ศึกษา ระหว่าง มกราคม 2564 ถึง ธันวาคม 2564 แล้วนำข้อมูลที่ได้ มาวิเคราะห์และสังเคราะห์รายละเอียดเนื้อหาของข้อมูลที่ แล้วนำมาเขียนบรรยายเชิงพรรณนา

ผลการวิจัย

วัตถุประสงค์ข้อที่ 1 สถานการณ์การเกิดภาวะวิกฤตจากการถูกโจมตี ระบบฐานข้อมูล โรงพยาบาลสระบุรี

สถานการณ์ที่ผิดปกติของระบบสารสนเทศเกิดขึ้นเมื่อเครื่องคอมพิวเตอร์ ของฝ่ายโภชนาการและ กลุ่มงานเภสัชกรรม ขัดข้อง ไม่สามารถสืบค้นประวัติผู้ป่วย และ และไม่สามารถบันทึกข้อมูลผู้ป่วยได้ เหมือนเดิม จึงแจ้งให้เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศที่ขึ้นเวรปฏิบัติงานให้แก้ไข ซึ่งจากการเข้าดำเนินการตรวจสอบเบื้องต้นตามคำบอกเล่าของผู้ให้ข้อมูลคนสำคัญสรุปได้ดังนี้

1. ระบบคอมพิวเตอร์เริ่มขัดข้องไม่สามารถใช้งานได้ปกติโดยเริ่มจากจากห้องจ่ายยาและ ฝ่ายโภชนาการ เจ้าหน้าที่ที่ขึ้นเวรปฏิบัติงานจึงเข้าไปตรวจสอบการทำงานพื้นฐานของเครื่องควบคุมแม่ข่ายจึงพบว่ามีการทำงานที่ผิดปกติ จึงรายงานไปยัง ผู้บริหารด้านเทคโนโลยีสารสนเทศเพื่อทราบและช่วยดำเนินการแก้ปัญหา

2. เมื่อตรวจสอบเชิงลึกพบว่า ระบบฐานข้อมูลถูกปิด และถูกเข้ารหัส ตรวจพบว่าไวรัสที่ทำการล๊อครหัสนามสกุล spade ทำให้ไม่สามารถเข้าถึงข้อมูลผู้ป่วยได้ รวมถึงข้อมูลที่อยู่ใน External Hard Disk ที่ สำรองไว้ จึงปิด Server ทุกตัว และปลด server ออกจากการเชื่อมต่อกับเครือข่ายของโรงพยาบาล ความเสียหายที่เกิดขึ้นพบว่ามีความเสี่ยงอยู่ในระดับสูงสุด (ระดับ5) (ชุษณะ มกรสาร และ วรรษา เปาอินทร์,2561)

3. ได้มีการแบ่งทีมการทำงานออกเป็น 2 ทีม คือ ทีมกู้ระบบ และ ทีมประสานงาน เพื่อคอยแจ้งข่าวสาร และ วางแผนในการให้บริการผู้ป่วย โดยนำระบบ Manual มาใช้ขณะที่รอระบบกลับคืนมา ตั้งหน่วยสื่อสารประชาสัมพันธ์ให้ประชาชนรับทราบสถานการณ์และแนวทางปฏิบัติเมื่อมาตรวจรักษาที่โรงพยาบาลสระบุรี

วัตถุประสงข้อที่ 2 เพื่อวิเคราะห์ภาวะวิกฤติของระบบสารสนเทศโรงพยาบาลสระบุรี

การหาวิเคราะห์เพื่อสาเหตุของการเกิดภาวะวิกฤติพบหลายประเด็นที่อาจเป็นสาเหตุของการถูกโจมตีจากผู้ไม่หวังดี โดยผู้เกี่ยวข้องได้เล่าถึงเหตุการณ์ที่พบก่อนถูกโจมตีสรุปได้ดังนี้

1. บุคลากรของโรงพยาบาลสระบุรีขาดความรู้ความเข้าใจในเรื่องของความปลอดภัยของระบบสารสนเทศ ไม่ใช่เฉพาะ ผู้ใช้งานแต่รวมไปถึงผู้ดูแลระบบด้วย เนื่องจากมีเครื่องคอมพิวเตอร์ของเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศคนหนึ่ง พบว่ามีโปรแกรมแปลกๆเกิดขึ้นในหน้าจอ จึงลบโปรแกรมนั้นออกโดยไม่เฉลียวใจว่าอาจเป็นสัญญาณอันตราย นอกจากนี้ยังพบว่า ช่วงต้นเดือนกันยายน พบไวรัสในไดร์Z: (ไดร์กลางสำหรับแชร์ข้อมูล) สำหรับผู้ใช้งาน มักจะเขียน Username และรหัสผ่านไว้ที่จอคอมพิวเตอร์ และ ไม่ค่อยเปลี่ยนรหัสผ่าน ตามที่นโยบายของโรงพยาบาลกำหนด โดยให้เหตุผลว่า ถ้าเปลี่ยนแล้ว จะจำรหัสใหม่ไม่ได้ และยังพบอีกว่าบางหน่วยงานติดตั้งโปรแกรมที่ต้องการใช้เอง

2. โรงพยาบาลสระบุรี มีการออกแบบระบบเครือข่าย (Network Security)ไม่มีความ มั่นคง สามารถเข้าถึงได้ง่ายเกินไป จึงเกิดภาวะวิกฤติ ขึ้น โดยเน้นให้ผู้ใช้งานมีความสะดวกและง่ายในการเข้าถึงสามารถ remote เข้ามาใช้งานได้ แม้จะอยู่ภายนอกโรงพยาบาล เพื่อจูงใจให้ เจ้าหน้าที่ของโรงพยาบาลหันมาใช้เทคโนโลยีแทนการใช้ข้อมูลในกระดาษ ประกอบกับคอมพิวเตอร์และอุปกรณ์ที่ใช้อยู่ ค่อนข้างล้าสมัย การใช้ระบบปฏิบัติการไม่ update ซึ่งอาจเป็นข้อจำกัดในเรื่องของ โปรแกรมของโรงพยาบาลใช้มานานมากกว่า 20 ปี จึงไม่รองรับระบบปฏิบัติการใหม่ๆ ที่ทันสมัย จึงควรหาวิธีหรือปรับเปลี่ยนวิธีให้มีความปลอดภัยมากขึ้น

3. ผู้รับผิดชอบขาดการควบคุมกำกับ ติดตาม หรือ บังคับและไม่มีบทลงโทษเมื่อมีผู้ใช้งานไม่ปฏิบัติตามนโยบายที่กำหนด

4. ประเด็นความความเสี่ยงที่สำคัญที่พบคือ ในเรื่องของการสำรองข้อมูลที่ทำอยู่ในปัจจุบันน่าจะมีจำนวนที่ไม่เพียงพอ ควรเพิ่มจำนวนชุดของการสำรองข้อมูล และควรมีสถานที่เก็บข้อมูลที่สำรองให้มีความปลอดภัย และเพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นในอนาคต โรงพยาบาลสระบุรีควรต้องหาผู้เชี่ยวชาญเข้ามาช่วยดูแล ทั้งในส่วนของ การวางระบบเครือข่าย และ การจัดการฐานข้อมูลเนื่องจากภาวะวิกฤตในครั้งนี้ ต้องขอความช่วยเหลือไปยังศูนย์ไซเบอร์กองทัพอากาศ และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) โดยใช้เวลา 2 สัปดาห์ในการกู้ระบบกลับคืนมา

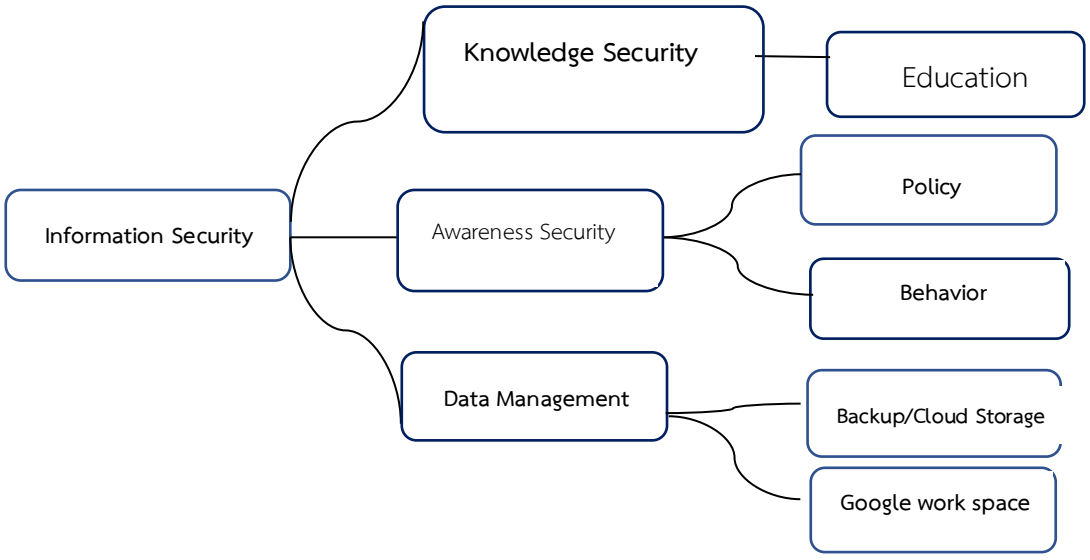
อภิปรายผลการวิจัย

ระบบสารสนเทศของโรงพยาบาลสระบุรีได้ผ่านกาลเวลามามากกว่ายี่สิบปี มีทั้งช่วงเวลาที่ระบบทำงานได้ไม่มีปัญหาและบางช่วงที่พบกับอุปสรรคและความท้าทาย ไม่ว่าจะเป็นระบบใด ย่อมต้องพบกับการเปลี่ยนแปลง เมื่อวิเคราะห์ สาเหตุจากการวิเคราะห์ข้อมูลจาการการสอบถาม ผู้ที่มีหน้าที่ดูแลรับผิดชอบระบบสารสนเทศ และผู้ที่มีส่วนเกี่ยวข้องโดยตรงกับระบบระบบสารสนเทศของโรงพยาบาลสระบุรีแล้ว พบว่า สถานการณ์การถูกโจมตีเริ่มเห็นสิ่งผิดปกติจากการใช้งานที่ติดขัดของหน่วยงาน ไม่กี่หน่วยงาน แล้วเริ่มลุกลาม ด้วยการล๊อคข้อมูลไม่ให้ผู้ใช้งานเข้าถึงข้อมูล สุดท้ายผู้รับผิดชอบทางด้านสารสนเทศของโรงพยาบาลสระบุรีต้องทำการปิดระบบทั้งหมดด้วยการตัดการเชื่อมต่อของเครื่องแม่ข่าย ทั้งภายในและ ภายนอกโรงพยาบาล สาเหตุที่นำไปสู่ภาวะภาวะวิกฤต สาเหตุหลักมาจากระบบเครือข่ายที่ออกแบบโดยเน้นความสะดวกของผู้ใช้งานเกินไป และการไม่ปรับอุปกรณ์และคอมพิวเตอร์ให้ทันสมัยมีความเสี่ยงต่อการถูกโจมตี การมีงบประมาณเพื่อพัฒนาเทคโนโลยีที่เข้มแข็งและทันสมัยจะทำให้ให้บรรลุเป้าหมายของความปลอดภัย สอดคล้องกับการศึกษาของ สุวรรณา เสมอเนตร (2562) และ Zwilling (2022) ที่พบว่า ภัยคุกคามทางไซเบอร์และผลกระทบต่อองค์กร การรับรู้ยังมีความสัมพันธ์กับเครื่องมือป้องกัน ดังนั้นบุคลากร ควรมีความรู้และสามารถรับรู้ถึงภัยคุกคามได้ องค์กรจำเป็นต้องมีกำลังคนงบประมาณและเทคโนโลยีที่เข้มแข็งเพื่อให้บรรลุเป้าหมายและเช่นเดียวกับการศึกษาของ จิตตกานต์ บุญศิริทิวัตถ์ และโกวิท รพีพิศาล (2560) ที่พบว่า ภัยคุกคามที่เกิดมากที่สุดคือ จากตัวบุคคล ข้อผิดพลาดทางเทคนิคของฮาร์ดแวร์ ข้อผิดพลาดทางเทคนิคของซอฟต์แวร์ และเทคโนโลยีล้าสมัย สำหรับในด้านความรู้เรื่อง network security และ cyber attack พบว่า บุคลากรทั้งในส่วนของผู้ดูแลระบบและผู้ใช้งาน ของโรงพยาบาลสระบุรีขาดความรู้ในเรื่องดังกล่าว ภัยคุกคามทางไซเบอร์ส่งผลกระทบต่อองค์กร ดังนั้นบุคลากร ควรมีความรู้ในเรื่องภัยคุกคามที่เพียงพอการฝึกอบรมและการรับรู้ เกี่ยวกับภัยคุกคามด้านความปลอดภัยของข้อมูลมีความจำเป็นเพื่อรับมือกับภัยคุกคามที่อาจเกิดขึ้น สอดคล้องกับการศึกษาของ Pérez-González et al.(2019) การศึกษาของ Hassandoust (2020) และการศึกษาของ นิตยปภา จันทะปัสสา (2562) ที่พบว่า ความรู้ด้านความปลอดภัยและการมองเห็นความปลอดภัยของข้อมูลตลอดจนแนวทางปฏิบัติขององค์กรด้านความปลอดภัยมีผลดีต่อประสิทธิภาพการจัดการความปลอดภัยของข้อมูลและควรมีการให้ความรู้อย่างสม่ำเสมอและต่อเนื่อง การฝึกอบรมและการรับรู้ เกี่ยวกับภัยคุกคามด้านความปลอดภัยของข้อมูลเพื่อการรับมือกับภัยคุกคามที่อาจเกิดขึ้น ในส่วนของความตระหนักถึงความปลอดภัยของสารสนเทศพบว่า ทั้งผู้ดูแลระบบและบุคลากรผู้ใช้งานไม่ตระหนักถึงภัยคุกคามทางไซเบอร์ เมื่อพบสิ่งผิดปกติเกิดขึ้นในคอมพิวเตอร์ที่ใช้งาน ไม่เฉลียวใจถึงสิ่งผิดปกติที่เกิดขึ้น มิได้สื่อสาร หรือ บอกกล่าวถึง ผลที่อาจเกิดขึ้น ตั้งรหัสผ่านไม่รัดกุม และไม่เปลี่ยนรหัสผ่านตามนโยบายที่กำหนด หลายการศึกษาพบว่า เหตุการณ์ด้านความปลอดภัยส่วนใหญ่เกิดขึ้นเนื่องจากการเพิกเฉยต่อความเสี่ยงหรือการประเมินที่ไม่ถูกต้อง เหตุการณ์ของภัยคุกคามที่เกิดขึ้น อาจเกิดจากการที่ผู้เชี่ยวชาญด้านความปลอดภัยไม่รับรู้ถึงภัยคุกคามอย่างครอบคลุม

สอดคล้องกับการศึกษาของ Turskis et al.(2019) การศึกษาของ Thangavelu, Krishnaswamy & Sharma, 2020) และการศึกษาของ Bada, Sasse & Nurse (2019) ที่พบว่า การสร้างความตระหนักจะเป็นปัจจัยที่อาจนำไปสู่ความสำเร็จด้านความปลอดภัยทางไซเบอร์ และการบริหารจัดการความปลอดภัยของข้อมูล โรงพยาบาลสระบุรีมีนโยบายชัดเจนในด้านการรักษาความปลอดภัยของข้อมูล แต่พบว่า ผู้มีหน้าที่รับผิดชอบขาการควบคุม ติดตาม บังคับและไม่มีบทลงโทษเมื่อไม่ปฏิบัติตามนโยบายที่กำหนด การอำนวยความสะดวกโดยการแชร์ไฟล์ในไดร์กลางที่กำหนดไว้ ทำให้เป็นแหล่งแพร่กระจายของไวรัสและการสำรองข้อมูลที่ทำอยู่ในปัจจุบันยังไม่ปลอดภัย และ มีจำนวนชุดสำรองไม่เพียงพอ ประกอบกับมีการเก็บข้อมูลสำรองไว้ในที่ไม่เหมาะสมทำให้เวลาเกิด Ransomware attack ข้อมูลที่สำรองไว้จึงถูกเข้ารหัสไปด้วยพร้อมกับฐานข้อมูลหลัก ควรมีแนวทางปฏิบัติขององค์กรด้านความปลอดภัยและวิเคราะห์ผลกระทบที่มีต่อประสิทธิภาพการจัดการความปลอดภัยของข้อมูล สอดคล้องกับการศึกษาของ Pérez-González et al. (2019) และการศึกษาของ Bada, Sasse & Nurse (2019) ที่พบว่า ความปลอดภัยมีผลดีต่อประสิทธิภาพการจัดการความปลอดภัยของข้อมูล เนื่องจากการจัดการความปลอดภัยและการจัดการเชิงรุกมีผลต่อการเพิ่มความสำเร็จด้านความปลอดภัย

องค์ความรู้ใหม่จากการวิจัย

จากการวิเคราะห์หาสาเหตุของการถูกโจมตีจาก Ransomware พบประเด็นที่สำคัญที่จะนำมาศึกษาต่อเพื่อยืนยันและหาวิธีการป้องกันมิให้เกิดเหตุการณ์ที่พลาดพลั้งขึ้นอีกในอนาคต คือ โรงพยาบาลสระบุรี ต้องมีการเสริมสร้างความรู้ด้านความปลอดภัยของสารสนเทศให้กับ บุคลากรทั้งในส่วนของผู้ดูแลระบบและบุคลากรผู้ใช้งาน ต้องสร้างความตระหนักในด้านความปลอดภัยและการใช้งานสารสนเทศให้มากยิ่งขึ้น ต้องมีวิธีการจัดการให้ฐานข้อมูลมีความปลอดภัยทั้งในส่วนของการสำรองข้อมูล การจัดเก็บ และ ที่สำคัญคือต้องสร้างแนวทางการปฏิบัติเพื่อให้บุคลากรทุกหน่วยมีพฤติกรรมที่เหมาะสมในการใช้สารสนเทศอย่างปลอดภัย มีการจัดการสารสนเทศที่มีประสิทธิภาพเพื่อเกิดประสิทธิผลให้กับสารสนเทศของโรงพยาบาลสระบุรีในอนาคต สถานการณ์และความเสี่ยงที่เกิดขึ้นและแนวทางเพื่อป้องกันการเกิดเหตุภาวะวิกฤตในอนาคต สรุปเป็น Diagram ดังแผนภาพที่ 1



แผนภาพที่ 1 Diagram of information Security system in Saraburi hospital

สรุป

สถานการณ์การเกิดภาวะวิกฤตของระบบสารสนเทศเกิดขึ้น เนื่องจากถูก Ransomware Void Crypt Spade โจมตี เบื้องต้นพบว่ามีไฟล์ข้อมูลเกี่ยวกับการรักษาพยาบาลเช่น ประวัติการรักษาพยาบาล รายการยาที่ผู้ป่วยได้รับ ประวัติที่สแกนไว้ ข้อมูลทั้งหมดถูกเข้ารหัส (Encrypt) พร้อมกับขึ้นข้อความเรียกร้องค่าไถ่แลกกับการถอดรหัส (Decrypt) โดยมิได้ระบุจำนวนค่าไถ่ที่ชัดเจน แต่ให้อีเมล์เพื่อติดต่อกลับไป การเข้ารหัสข้อมูลได้แพร่กระจายไปยังข้อมูลส่วนที่มีการสำรองไว้ เป็นเหตุให้ระบบและข้อมูลสารสนเทศของโรงพยาบาลไม่สามารถใช้งานได้ตามปกติ จึงปรับเปลี่ยนการใช้ข้อมูลสารสนเทศและเส้นทางเดินเอกสารเป็นระบบ Manual ทดแทนระบบอิเลคทรอนิกส์ ใช้เวลา 2 สัปดาห์ ในการกู้ฐานข้อมูลกลับคืนมาโดยทีมของศูนย์ไซเบอร์กองทัพอากาศ และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) สำหรับสาเหตุที่นำไปสู่ความเสี่ยงที่ทำให้ถูกโจมตีจาก Ransomware โดยผลของการสัมภาษณ์เชิงลึก (In-Depth Interview) พบว่า สาเหตุที่สำคัญมาจาก บุคลากรขาดความรู้ความเข้าใจของความปลอดภัยของระบบสารสนเทศ บุคลากรขาดการตระหนักด้านความปลอดภัยของสารสนเทศ โดยเมื่อพบสิ่งผิดปกติเกิดขึ้นในคอมพิวเตอร์ที่ใช้งานของตนเอง ไม่เฉลียวใจถึงสิ่งผิดปกติที่เกิดขึ้น มิได้สื่อสาร หรือ บอกกล่าวถึง ผลที่อาจเกิดขึ้น ในเรื่องการออกแบบระบบเครือข่าย (Network Security) มีการออกแบบระบบเพื่อให้สะดวก และง่ายต่อการเข้าถึงฐานข้อมูล ด้วยเหตุผลเพื่อจูงใจให้บุคลากรใช้งานในระบบสารสนเทศ อุปกรณ์ที่ใช้อยู่ล้าสมัย ขาดการ Up date ระบบปฏิบัติการ ทำให้มีช่องโหว่ด้านความปลอดภัย ในส่วนของการจัดการด้านความปลอดภัยของข้อมูล (Data Security) ขาดการควบคุมติดตามการบังคับและไม่มีบทลงโทษเมื่อไม่ปฏิบัติตามนโยบายที่กำหนด การแชร์ไฟล์ในไดร์กลางที่ กำหนดไว้ ทำให้เป็นแหล่งแพร่กระจายของไวรัส การสำรองข้อมูลที่ทำอยู่ในปัจจุบันยังไม่ปลอดภัย และมีจำนวนที่ไม่เพียงพอ และอยู่ในที่ที่ไม่เหมาะสมทำให้เวลาเกิด Ransomware attack ข้อมูลที่มีการสำรองไว้จึงถูกเข้ารหัสไปพร้อมกับฐานข้อมูลหลัก

ข้อเสนอแนะ

ข้อเสนอแนะในการนำผลการวิจัยไปใช้ประโยชน์

1. ผลการศึกษาที่ได้จะช่วยให้ผู้ที่มีส่วนเกี่ยวข้อง และผู้ใช้งานระบบสารสนเทศ มีความระมัดระวังในการใช้งานสารสนเทศมากยิ่งขึ้น

2. เป็นแนวทางในการป้องกันและการตั้งรับก่อนจะเกิดเหตุการณ์ที่ไม่คาดคิด เมื่อพบเห็นเหตุการณ์ที่ผิดปกติในระบบสารสนเทศ

ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

ประเด็นที่สำคัญที่ควรจะไปศึกษาเพื่อยืนยันและหาวิธีการป้องกันมิให้เกิดเหตุการณ์ที่พลาดพลั้งขึ้นอีกในอนาคต คือ

1. ควรมีการศึกษาวิจัยเชิงปริมาณเพื่อทดสอบความเกี่ยวข้อง หรือ อิทธิพลของการเสริมสร้างความรู้ด้านความปลอดภัยของสารสนเทศ ความตระหนักในด้านความปลอดภัยการใช้งานสารสนเทศ การจัดการให้ฐานข้อมูลมีความปลอดภัยและพฤติกรรมที่เหมาะสมในการใช้สารสนเทศอย่างปลอดภัยว่าส่งผลทางตรงหรือทางอ้อมอย่างไรบ้าง ต่อยอดในกลุ่มของ ผู้ใช้งานในระบบสารสนเทศ ทั้งผู้ให้บริการและประชาชนผู้รับบริการเพื่อเป็นแนวทางในการป้องกันการเกิดภัยคุกคามกับระบบสารสนเทศ

2. ควรมีการศึกษา สร้างแนวทางการปฏิบัติงานเพื่อสร้างความปลอดภัยของระบบสารสนเทศ โดยให้ผู้ที่เกี่ยวข้องมีส่วนร่วมในการดำเนินการ

เอกสารอ้างอิง

จิตตกานต์ บุญศิริทิวัตถ์ และ โกวิท รพีพิศาล. (2560). การพัฒนาแนวทางในการจัดการความมั่นคงความปลอดภัยระบบสารสนเทศที่เหมาะสมของโรงพยาบาลเอกชนในกรุงเทพมหานคร. *รังสิตสารสนเทศ, 23* (1), 61-90.

จิรพล สังข์โพธิ์. (2560). *แผนปฏิบัติการดิจิทัลของกระทรวงแรงงานและสำนักงานปลัดกระทรวงแรงงาน ระยะ 5 ปี* พ. ศ.2560-2564. กรุงเทพฯ: สำนักงานปลัดกระทรวงแรงงาน.

ชุษณะ มะกรสาร และ วรรษา เปาอินทร์. (2561). *แนวทางการพัฒนาคุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาล.* กรุงเทพฯ: สมาคมเวชสารสนเทศไทย.

นิตยปภา จันทะปัสสา. (2562). *การพัฒนาระบบสารสนเทศการบริหารงานบุคคล โรงเรียนบ้านดอนตูมดอนโด* สำนักงานเขตพื้นที่การศึกษาประถมศึกษา มหาสารคาม เขต 1, *วารสารวิชาการและวิจัย มหาวิทยาลัยภาคตะวันออกเฉียงเหนือ, 9*(1), 82-89

พลากร ลาภอลงกรณ์. (2555). *สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)* สืบค้นเมื่อ 16 มกราคม 2565 จาก https://www.dga.or.th/

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

วศินี หนุนภักดี. (2562*). การวิเคราะห์ความเสี่ยงของผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของหน่วยงานภาครัฐในยุคเศรษฐกิจดิจิทัล. วารสารวิชาการบัณฑิตวิทยาลัยสวนดุสิต*, 13(2), 173-187.

ศิวลีย์ สิริโรจน์บริรักษ์. (2559). *การรักษาความมั่นคงปลอดภัยไซเบอร์. วารสารสถาบันชาการป้องกันประเทศ*, 6(3), 19-29.

สุวรรณา เสมอเนตร. (2562). *การพัฒนาระบบบริหาร ความมั่นคงปลอดภัยสารสนเทศภายใต้มาตรฐาน ISO/IEC 27001: 2013* ศูนย์ปฏิบัติการ Ministry of Public Health Internet Data Center (MOPH IDC). *วารสารวิชาการสาธารณสุข*, *28*(1), 117-132.

อดิศักดิ์ ถีระแก้ว ปุญชรัศมิ์ ศักดิ์ธรรมเจริญ และคณะ. (2561). *ประสิทธิผล และความพึงพอใจของการให้ความรู้แก่ผู้ป่วยต่อการใช้เอกสารอิเล็กทรอนิกส์ ร่วมกับเอกสารคำแนะนำสำหรับผู้ป่วยมะเร็ง ที่รับการรักษาด้วยรังสี. Journal of Thai Association of Radiation Oncology*, *24*(1), 14-24.

อนันต์ ชูยิ่งสกุลวิทย์. (2562). ระบบพัฒนาสมรรถนะด้านเทคโนโลยีสารสนเทศ และการสื่อสารเพื่อความมั่นคงปลอดภัยของสารสนเทศ. *วารสารสนเทศศาสตร์*, *37*(3), 59-80.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). *Cyber security awareness campaigns: Why do they fail to change behaviour?.* arXiv preprint arXiv:1901.02672.

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

Brewer, R. (2017). *Ransomware attacks: detection, prevention and cure*. Network Security, 9, 5-9.

Choo, C. W., & de Alvarenga Neto, R. C. D. (2010). Beyond the ba: Managing enabling contexts in knowledge organizations. *Journal of Knowledge Management, 14*(4), 592-610.

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). Massachusetts: 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.

Nader Sohrabi Safa, 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.

Pérez-González, D., Preciado, ST, & Solana-Gonzalez, P. (2019). *Organizational practices as antecedents of the information security management performance: An empirical investigation*. United Kingdom: Emerald Publishing.

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.

Turskis, Z., Goranin, N., Nurusheva, A., & Boranbayev, S. (2019). Information security risk assessment in critical infrastructure: a hybrid MCDM approach. *Informatica, 30*(1), 187-211.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: a comparative study. *Journal of Computer Information Systems, 62*(1), 82-97.