การจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ : บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

Government Agencies' Cyber Threat Risk Management : Lessons Learned from Judicial Agencies under the Jurisdiction of the Chief Justice Region 9

ธนพงศ์ ฉันทวิเชียร Thanaphong Chanthawichian[1]

สมพร คุณวิชิต Somporn Khunwishit[2]

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อ (1) วิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยง และแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 (2) ศึกษาความสำเร็จและอุปสรรคในการดำเนินงานด้านการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ และ (3) เพื่อเสนอแนะแนวทางการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในอนาคต สำหรับหน่วยงานดังกล่าว ใช้ระเบียบการวิจัยเชิงคุณภาพ โดยการศึกษาค้นคว้าเอกสารและการสัมภาษณ์เชิงลึก เก็บข้อมูลจากผู้ให้ข้อมูลหลักทั้งสิ้น 36 คน ได้แก่ เจ้าหน้าที่ผู้ดูแลระบบและเจ้าหน้าที่ผู้ปฏิบัติงานศาล จากนั้นนำข้อมูลมาวิเคราะห์โดยใช้เทคนิคการสร้างข้อสรุปแบบอุปนัย

ผลการศึกษา พบว่า ปัจจัยเสี่ยงจากภัยคุกคามไซเบอร์ มีอยู่ 5 ประเภท ได้แก่ การใช้โปรแกรมประยุกต์ที่ถูกดาวน์โหลด การใช้เครือข่ายไร้สาย สภาพแวดล้อมที่ล่อแหลม การโจมตีแบบไม่ตั้งใจ และการโจมตีแบบตั้งใจ ความสำเร็จของการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานดังกล่าว ได้แก่ มีการกำหนดระดับการเข้าถึงข้อมูลและการป้องกันการเข้าระบบโดยไม่พึงประสงค์ ข้อมูลมีความถูกต้อง ครบถ้วนแม่นยำ และฮาร์ดแวร์และซอฟต์แวร์อยู่ในสภาพพร้อมใช้งานและพร้อมป้องกันจากภัยคุกคามไซเบอร์ ส่วนอุปสรรคของการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ ได้แก่ งบประมาณในการจัดหาฮาร์ดแวร์และซอฟต์แวร์ยังไม่เพียงพอ บุคลากรยังขัดความรู้และทักษะการจัดการความเสี่ยงไซเบอร์ จำนวนบุคลากรทางไซเบอร์ที่มีไม่เพียงพอ ที่ตั้งของศาลที่อยู่ใกล้ทะเลทำให้มีความเสี่ยงได้รับผลกระทบต่อฮาร์ดแวร์ทำให้เกิดความเสียหาย และระบบที่เกิดขึ้นใหม่เป็นระบบงานซ้ำซ้อนที่มีอยู่เดิม ข้อเสนอแนะแนวทางการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในอนาคต ได้แก่ เพิ่มการจัดสรรงบประมาณสำรวจประเมินความเสี่ยงของฮาร์ดแวร์และซอฟต์แวร์รวมทั้งการต่อประกันอุปกรณ์เครือข่าย จัดอบรมพัฒนาทักษะ

[1] นักศึกษาระดับปริญญาโท หลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์

E-mail: tanapong.tc@gmail.com

[2] รองศาสตราจารย์ ดร. ภาควิชารัฐประศาสนศาสตร์ คณะวิทยาการจัดการ มหาวิทยาลัยสงขลานครินทร์

E-mail: somporn.kh@psu.ac.th

เจ้าหน้าที่ผู้ดูแลระบบและเจ้าหน้าที่ ขออัตรากำลังเพิ่มเติมหรือใช้บุคลากรทางไซเบอร์ร่วมกันในการแก้ไขปัญหา ควรปรับเปลี่ยนนโยบายที่ตั้งศาลที่อยู่ใกล้ทะเลหรือควรออกแบบอาคารและวัสดุในการปกป้องอุปกรณ์ ครุภัณฑ์ต่างๆ ไม่ให้เกิดความเสียหายหากศาลตั้งอยู่ใกล้ทะเล และสุดท้าย ควรพัฒนาระบบงานใหม่ไม่ให้เกิดความซ้ำซ้อน

คำสำคัญ : ภัยคุกคามไซเบอร์, การจัดการความเสี่ยงไซเบอร์, หน่วยงานศาลยุติธรรม, การบริหารจัดการภาครัฐ

ABSTRACT

The purposes of this research are to (1) analyze threats, risk factors, and current practices of cyber threat risk management among judicial agencies under the jurisdiction of the Chief Justice Region 9; (2) examine the success and obstacles of cyber threat risk management; and (3) provide suggestions for better management of cyber threat risk in the future. Qualitative research methods were employed. Data were gathered through documentary research and in-depth interviews. The 36 participants who served as key informants in this study consisted of representatives from the judicial agencies under the jurisdiction of the Chief Justice Region 9. Data were verified using the data triangulation method, and after that, data were analyzed inductively.

Results reveal that cyber threat risk factors faced by these agencies include the free-downloaded program software, wireless internet connection, exposed environment, unintentional attack and intentional attack. The successes of cyber threat risk management among these agencies include the establishment of accessibility levels, correctness of data, accuracy of data, and the readiness for preventing cyber threat for both software and hardware. Results also show that they are 5 obstacles that hampered the management of cyber threat risk among these agencies, which include inadequate budget for software and hardware procurement, the lack of knowledge and skill regarding cyber threat risk management among personnel, the insufficiency of IT or cyber personnel, the locations of judicial agencies that are near the coasts, and the new systems that are often redundant with the existing systems. It is recommended in this research that judicial agencies allocate more budget to assess risk in both software and hardware and to purchase insurance for connection equipment, train personnel about cyber treat risk

management, request for more IT or cyber personnel, change location from coastal areas and reduce redundancy of systems.

Keyword : Cyber Threat, Cyber Threat Risk Management, Judicial Agencies, Public Administration

บทนำ

บทบาทและความสำคัญของเทคโนโลยีได้มีการพัฒนาอย่างต่อเนื่อง ทำให้สภาพของสังคมเปลี่ยนเป็นยุคดิจิทัล ประเทศไทยต้องปรับเปลี่ยนให้ทันกับเทคโนโลยีที่มีความเปลี่ยนแปลง โดยมีการกำหนดกรอบและแนวทางพัฒนาให้หน่วยงานของรัฐทุกภาคส่วนต้องปฏิบัติตาม เพื่อให้บรรลุวิสัยทัศน์ประเทศไทย ภายใต้แผนยุทธศาสตร์ชาติ 20 ปี โดยระบบราชการเป็นกำลังสำคัญในการขับเคลื่อนนโยบายให้บรรลุตามวัตถุประสงค์ รวมถึงศาลยุติธรรมที่จะต้องดำเนินงานเพื่อให้สอดคล้องกับนโยบายของรัฐที่ต้องการขับเคลื่อนประเทศไทยให้มีความก้าวหน้าทางเทคโนโลยีดังกล่าว ถึงแม้ศาลยุติธรรมจะมีการพัฒนาระบบทั้งในส่วนฮาร์ดแวร์และซอฟต์แวร์ อย่างไรก็ตามในปี 2559 เว็บไซต์ศาลยุติธรรมถูกเจาะระบบ ซึ่งสำนักเทคโนโลยีสารสนเทศ (2559) ได้ตรวจพบการทำงานของเครื่องคอมพิวเตอร์ข่ายที่ให้บริการเว็บไซต์หน่วยงานศาลยุติธรรมทั่วประเทศมีการทำงานที่ผิดปกติ สาเหตุที่ถูกเจาะระบบผ่านช่องโหว่ของเว็บไซต์ศาลยุติธรรมพบว่ามีผู้ไม่หวังดีพยายามชัดขวางการทำงานหรือเจาะระบบ (โจมตีในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการเว็บไซต์หน่วยงานศาลทั่วประเทศ โดยใช้วิธี Denial Of Service (Dos) ส่งผลทำให้เว็บไซต์ศาลยุติธรรมทั่วประเทศใช้งานไม่ได้ รวมถึงต้องปิดระบบต่างๆ ภายในของศาลยุติธรรม เนื่องจากมีกลุ่มแฮกเกอร์ที่ไม่พึงพอใจในการตัดสินคดีเกาะเต่าของศาลจังหวัดสมุย

ดังนั้นการจัดการความเสี่ยงจึงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญ โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร ด้วยเหตุนี้จึงได้ทำการศึกษาถึงการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ บทเรียนจากหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 เพื่อได้แนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ และเป็นข้อมูลประกอบการสนับสนุนฮาร์ดแวร์และซอฟต์แวร์เพื่อลดความเสี่ยงจากภัยคุกคามด้านไซเบอร์ได้อย่างเหมาะสม และมีความมั่นคงปลอดภัยทันต่อการเปลี่ยนแปลงของโลกไซเบอร์ในปัจจุบัน

ฉะนั้น จากความจำเป็นข้างต้นจึงนำมาสู่การวิจัยครั้งนี้ โดยมีวัตถุประสงค์ของการศึกษา คือ

1. เพื่อศึกษาวิเคราะห์ภัยคุกคาม ปัจจัยความเสี่ยงและแนวปฏิบัติในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

2. เพื่อศึกษาความสำเร็จและอุปสรรคในการดำเนินงานด้านการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

3. เพื่อเสนอแนะแนวทางการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ในอนาคตสำหรับหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

ทบทวนวรรณกรรม และการพัฒนาสมมติฐาน

แนวคิดเกี่ยวกับภัยคุกคามไซเบอร์

ภัยคุกคามทางไซเบอร์ (Cyber Threat) หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, 2562; ประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่องหลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันวินาศภัย พ.ศ. 2563, 2563; ยุทธศักดิ์ รักเสรีพิทักษ์ และ ศิริลักษม์ ตันตยกุล, 2565) ซึ่งสรุปการแบ่งประเภทภัยคุกคามทางไซเบอร์ได้ 4 ประเภท วิศณุ สร้างวงศ์ใหม่ (2561) ณรงค์เวตย์ เรืองจวง (2561) (1) ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์ที่ถูกดาวน์โหลดหรือได้มาจากสื่ออุปกรณ์อื่นเพื่อติดตั้งบนคอมพิวเตอร์หรืออุปกรณ์โทรศัพท์เคลื่อนที่ (2) ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์หลอกที่ออกแบบมาให้เหมือนของจริง (3) ภัยคุกคามจากการใช้เครือข่ายไร้สาย (4) ภัยคุกคามที่เกิดจากการโจมตีแบบเจาะจงเป้าหมาย

แนวคิดเกี่ยวกับการจัดการความเสี่ยง

การจัดการความเสี่ยง (Risk Management) คือ กระบวนการดำเนินงานหรือการกำหนดวิธีการจัดการที่เหมาะสมขององค์กร ขั้นตอนที่เป็นระบบและมีความต่อเนื่องอย่างเหมาะสม เพื่อลดเหตุของความเสี่ยงที่เกิดขึ้นหรือโอกาสของเหตุการณ์ที่เกิดในอนาคตให้อยู่ในระดับที่องค์กรยอมรับได้ มีการประเมิน ควบคุม และตรวจสอบอย่างเป็นระบบ เพื่อให้เกิดความเชื่อมั่นต่อองค์กร เป็นภาพลักษณ์ที่ดีขององค์กร จิรพร สุเมธีประสิทธิ์ และคณะ (2556 อ้างถึงใน ญาณิศา เผื่อนเพาะ, 2562) ได้กล่าวว่า เป้าหมายของความเสี่ยงมี 4 ประเภท คือ (1) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) เป็นความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ แผนการดำเนินงาน และการนำไปปฏิบัติไม่เหมาะสมกับปัจจัยภายในองค์กร และสภาพแวดล้อมภายนอก (2) ความเสี่ยงด้านการปฏิบัติการ (Operational Risk) เป็นความเสี่ยงที่เกิดจากการดำเนินงานที่อาจเกิดข้อผิดพลาดขึ้นจากการบริหารงาน และระบบงานขององค์กร (3) ความเสี่ยงด้าน

การเงิน (Financial Risk) เป็นความเสี่ยงที่เกี่ยวข้องกับด้านการเงินทั้งหมด เช่น สภาพคล่องทางการเงิน ความน่าเชื่อถือทางบัญชี อัตราแลกเปลี่ยนเงินตรา เป็นต้น (4) ความเสี่ยงด้านการปฏิบัติตามกฎเกณฑ์ (Compliance Risk) เป็นความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติตามกฎระเบียบและกฎหมาย

องค์ประกอบของการจัดการความเสี่ยง ERM (Enterprise Risk Management) 8 ประการ ได้แก่ (1) สภาพแวดล้อมภายในองค์กร (Internal Environment) สภาพแวดล้อมขององค์กรเป็นองค์ประกอบที่สำคัญในการกำหนดกรอบการจัดการความเสี่ยง (2) การกำหนดวัตถุประสงค์ (Objective Setting) องค์กรต้องกำหนดวัตถุประสงค์ในการจัดการความเสี่ยงให้สอดคล้องกับกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้ (3) การบ่งชี้เหตุการณ์ (Event Identification) เป็นการรวบรวมเหตุการณ์ที่อาจเกิดขึ้นจากปัจจัยเสี่ยงทั้งภายในและภายนอกองค์กร (4) การประเมินความเสี่ยง (Risk Assessment) การประเมินความเสี่ยงเป็นการจำแนกและจัดลำดับความสำคัญความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด และผลกระทบ (5) การจัดการความเสี่ยง หรือ การตอบสนองความเสี่ยง (Risk Response) เป็นการนำความเสี่ยงมาดำเนินการตอบสนองด้วยวิธีการที่เหมาะสม เพื่อลดความสูญเสียหรือผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้ (6) กิจกรรมการควบคุม (Control Activities) การกำหนดกิจกรรมและการปฏิบัติต่างๆ ที่กระทำเพื่อลดความเสี่ยง และทำให้การดำเนินงานบรรลุตามวัตถุประสงค์และเป้าหมายขององค์กร (7) สารสนเทศและการสื่อสาร (Information and Communication) องค์กรจะต้องมีระบบสารสนเทศและการติดต่อสื่อสารที่มีประสิทธิภาพ เป็นการบริหารความเสี่ยงให้เป็นไปตามกรอบ และขั้นตอนการปฏิบัติที่องค์กรกำหนด (8) การติดตามประเมินผล (Monitoring) องค์กรจะต้องมีการติดตามผลเพื่อให้ทราบถึงผลการดำเนินการว่ามีความเหมาะสมและสามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพหรือไม่

แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (2562) ความมั่นคงปลอดภัยไซเบอร์ หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

องค์ประกอบ Framework Core Functions แบ่งย่อยออกเป็นกรอบงานหลัก 5 functions ซึ่งเป็นกิจกรรมงานหลักด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ได้แก่ (1) Identify เป็นการพัฒนาความเข้าใจของหน่วยงานเกี่ยวกับการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้หน่วยงานสามารถมุ่งเน้นและจัดลำดับความสำคัญให้สอดคล้องกับกลยุทธ์การบริหารความเสี่ยงและความต้องการ (2) Protect การพัฒนาและจัดทำการป้องกันที่เหมาะสมเพื่อให้แน่ใจว่าหน่วยงานได้รับการปกป้อง เพิ่มความสามารถในการจำกัดหรือยับยั้งผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ความมั่นคงปลอดภัย

ไซเบอร์ ซึ่งมีการพัฒนาและจัดทำการป้องกัน (3) Detect หน่วยงานมีการพัฒนาและจัดทำกิจกรรมในการระบุเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้น ทำให้สามารถตรวจพบเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ได้ทันท่วงที (4) Respond ในส่วนการพัฒนาและจัดทำกิจกรรมเพื่อดำเนินการเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ทำให้สามารถยับยั้งผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (5) Recover ในการพัฒนาและจัดทำกิจกรรมเพื่อวางแผน เตรียมรับมือและกู้คืนการระบบต่างๆ เพื่อให้ระบบบริการที่เสียหายจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ทำให้สามารถกู้คืนการปฏิบัติงานให้กลับเป็นปกติได้ทันท่วงที เพื่อลดผลกระทบที่เกิดจากเหตุการณ์ภัยคุกคามไซเบอร์ NIST (2014 อ้างถึงใน ปริญญา หอมอเนก และACIS Research LAB, 2557; 2014 อ้างถึงใน วิลาส วิถีไพร, 2561)

แนวคิดการบริการสาธารณะและการให้บริการสาธารณะหน่วยงานศาลยุติธรรม

การบริการสาธารณะ เป็นกิจกรรมที่หน่วยงานที่มีอำนาจหน้าที่ที่เกี่ยวข้องที่อาจเป็นหน่วยงานของรัฐหรือเอกชนเป็นผู้ดำเนินการให้แก่ประชาชนผู้มารับบริการ ทั้งนี้โดยมีเป้าเหมาย ที่สำคัญคือการให้บริการที่ตอบสนองความต้องการของประชาชนอย่างทั่วถึงและเสมอภาค โดยหน่วยงานที่ให้บริการจะต้องส่งมอบบริการแก่ประชาชนด้วยจิตสำนึกที่ดีในการให้บริการ และมีการนำผลสะท้อนกลับจากประชาชนในฐานะผู้มาใช้บริการ เพื่อนำมาปรับปรุงพัฒนาการให้บริการให้มีประสิทธิภาพ ไม่ว่าจะเกี่ยวข้องกับข้อร้องเรียน ข้อเสนอแนะ ต่างๆ ทั้งนี้อาจกล่าวได้ว่า การบริการสาธารณะจำเป็นต้องคำนึงถึงคุณภาพและประสิทธิภาพของการให้บริการ โดยอาศัยเทคนิควิธีการที่หมาะสมต่อกลุ่มเป้าหมายที่ให้บริการ ช่วงเวลาและสถานที่การให้บริการ

การให้บริการของศาลถือเป็นภารกิจด้านการยุติธรรมที่รัฐต้องจัดทำเพื่ออำนวยความยุติธรรมให้กับประชาชนทุกคนอย่างเสมอภาค และบริหารจัดการบริการของศาลให้มีประสิทธิภาพและปรับปรุงเปลี่ยนแปลงบริการให้เหมาะสมกับสถานการณ์ และทันกับความต้องการของประชาชน ศาลยุติธรรมได้ให้ความสำคัญกับโดยพัฒนาการบริหารจัดการบริการของศาล และเป็นการเพิ่มโอกาสเพื่อให้ประชาชนผู้มาใช้บริการสามารถเข้าถึงศาลได้อย่างทั่วถึง และส่งเสริมความรู้ความเข้าใจเกี่ยวกับบทบาทและหน้าที่ของศาลยุติธรรม และความสัมพันธ์ระหว่างศาลและประชาชน

งานวิจัยที่เกี่ยวข้อง

ด้านการบริหารความเสี่ยง จากงานวิจัยทั้ง 2 เรื่อง พบว่าการบริหารความเสี่ยงช่วยให้ฝ่ายบริหารสามารถจัดการกับความไม่แน่นอนและความเสี่ยงของโอกาสได้อย่างมีประสิทธิผล ทำให้การดำเนินงานขององค์กรอยู่ในระดับความเสี่ยงที่ยอมรับได้ ได้แก่ ธีระศักดิ์ เปี่ยมสุภัคพงศ์, ธีระรัตน์ เปี่ยมสุภัคพงศ์, พรพรรณ สุวรรณประทีป, สุกานดา โรจนประภายนต์ และ วัฒนา เสรีคุณากุล (2561) ศึกษาการ

เรียนรู้เพื่อรับมือกับการบริหารความเสี่ยงของธุรกิจในบริบทใหม่ยุคอุตสาหกรรม 4.0 วิจิตรา สีแดงก่ำ (2562) ศึกษาการบริหารความเสี่ยงขององค์กรในศตวรรษที่ 21

ด้านปัจจัยสาเหตุและผลลัพธ์การจัดการความเสี่ยง จากงานวิจัยทั้ง 2 เรื่อง พบว่าองค์กรสามารถคิดปัจจัยสาเหตุและผลลัพธ์ และนำไปสู่กระบวนการจัดการความเสี่ยงซึ่งส่งผลต่อผลลัพธ์ในการบริหารจัดการความเสี่ยงได้อย่างดี เป็นสิ่งที่อยู่ในเกณฑ์ขององค์กรยอมรับได้ ได้แก่ สุฏิกา รักประสูติ (2558) ศึกษาบทบาทของผู้ตรวจสอบภายในต่อการจัดการความเสี่ยงองค์กร: ปัจจัยสาเหตุและผลลัพธ์ พิชญาพร พีรพันธุ์ และ วิโรจน์ เจษฎาลักษณ์ (2564) ศึกษากรอบแนวคิดปัจจัยเชิงสาเหตุและผลลัพธ์ของความสามารถในการจัดการความเสี่ยงขององค์กร

ด้านความมั่นคงปลอดภัยไซเบอร์ จากงานวิจัยทั้ง 5 เรื่อง พบว่าองค์กรควรจะมีมาตรการในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ โดยมีการสร้างความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่ เตรียมความพร้อมทั้ง ฮาร์ดแวร์และซอฟต์แวร์ ในการปกป้องภัยคุกคาม การพัฒนาทั้งบุคลากร แอพพลิเคชั่น ได้แก่ ปริญญา หอมอเนก และ ACIS Research LAB (2557) ศึกษาบทวิเคราะห์กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ระดับโลก อรรคเดช ประทีปอุษานนท์ และ ธาราทิพย์ กัลยาณมิตร (2560) ศึกษาแนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ วิศณุ สร้างวงศ์ใหม่ (2561) ศึกษาการเป็นมืออาชีพในการรักษาความปลอดภัยไซเบอร์ กริน ธัญญวิกร และ ชฎาภรณ์ สิงห์แก้ว (2564) ศึกษาบทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม อนาวิล แก้วสะอาด และ ณัฐวี อุตกฤษฎ์ (2564) ศึกษาเรื่องการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร

ด้านความตระหนักรู้และภัยคุกคามทางไซเบอร์ จากงานวิจัยทั้ง 4 เรื่อง พบว่าองค์กรควรต้องมีบุคลากรที่มีความรู้และความเข้าใจจากภัยคุกคามไซเบอร์ เพื่อที่จะได้ปฏิบัติงานได้อย่างปลอดภัย ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ได้แก่ ฝ่ายวิเคราะห์เทคโนโลยีป้องกันประเทศ สถาบันเทคโนโลยีป้องกันประเทศ (2559) ศึกษาภัยคุกคามทางไซเบอร์ ภาณุพล บรรณกิจโสภณ (2560) ศึกษาแนวโน้มภัยคุกคามด้านเทคโนโลยีสารสนเทศของกองทัพไทย นริส อุไรพันธ์ และ ธรนี มณีศรี (2563) ศึกษาโมเดลสมการเชิงโครงสร้าง เพื่อวิเคราะห์ปัจจัยที่ส่งผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชนสำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย เมธาพร ธรรมศิริ และ ศิรภัสสรศ์ วงศ์ทองดี (2565) ศึกษาความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร

ด้านการพัฒนาบุคลากร พัฒนาแอพพลิเคชั่นและการปรับปรุงอุปกรณ์ จากงานวิจัยทั้ง 6 เรื่อง พบว่าองค์กรควรต้องมีการพัฒนาทั้งทางด้านสมรรถนะบุคลากร แอพพลิเคชั่น และการปรับปรุง

อุปกรณ์ให้มีความทันสมัย จะส่งผลให้สามารถรักษาความปลอดภัยให้กับระบบได้ เป็นการเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ให้กับองค์กร ได้แก่ ปรัชญา เฉลิมวัฒน์ (2560) ศึกษาแนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อพร้อมรับภัยคุกคามระดับชาติ เกียรติศักดิ์ ลุยทอง (2561) ศึกษาการพัฒนาระบบตรวจสอบ เฝ้าระวัง และแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก ณรงค์เวตย์ เรืองจวง (2561) ศึกษาแนวทางการพัฒนาขีดความสามารถบุคลากร ด้านไซเบอร์ของกองทัพอากาศ ธนภัทร กิตติวณิชพันธุ์ และ อานนท์ ทับเที่ยง (2561) ศึกษาสมรรถนะของบุคลากรในหน่วยงานราชการด้านความมั่นคงปลอดภัยไซเบอร์ตามข้อกำหนด NIST และ มาตรฐาน ISO27001/2013 วิลาส วิถีไพร (2561) ศึกษาการพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง สุวันต์นา เสมอเนตร (2561) ศึกษาการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศภายใต้มาตรฐาน ISO/IEC 27001:2013 ศูนย์ปฏิบัติการ Ministry of Public Health Internet Data Center (MOPH IDC)

ด้านสถานภาพความพร้อมและดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ จากงานวิจัยทั้ง 2 เรื่อง พบว่าองค์กรควรต้องมีความพร้อมในการป้องกันและแก้ไขภัยคุกคามทางไซเบอร์ และความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจะได้จัดการกับความเสี่ยงต่างๆ จากภัยคุกคามไซเบอร์ได้อย่างดีและเป็นที่ยอมรับได้ขององค์กร รวมถึงการคืนสภาพกลับมาทำงานได้อีกโดยเร็ว ได้แก่ สุภาพร พรมโส, ปราลี มณีรัตน์ และ ประสงค์ ประณีตพลกรัง (2564) ศึกษาสถานภาพความพร้อมและดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ ยุทธศักดิ์ รักเสรีพิทักษ์ และ ศิริลักษม์ ตันตยกุล (2565) ศึกษาบทบาทของกองทัพกับนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อป้องกันภัยคุกคามรูปแบบใหม่

วิธีการดำเนินการวิจัย

เป็นงานวิจัยเชิงคุณภาพ เก็บข้อมูลโดยจากเอกสารต่างๆ ที่เกี่ยวข้อง วารสารวิชาการ และงานวิจัยที่เกี่ยวข้อง และการสัมภาษณ์เชิงลึก โดยกลุ่มผู้ให้ข้อมูลหลัก ทั้งหมด 36 คน ซึ่งเป็นเจ้าหน้าที่ผู้ดูแลระบบ 18 คน และเป็นเจ้าหน้าที่ผู้ปฏิบัติงานศาล 18 คน ทั้งนี้เกณฑ์การคัดเลือกผู้ให้ข้อมูลหลักประกอบด้วย ต้องมีคุณสมบัติสอดคล้อง โดยแบ่งออกเป็น 2 กลุ่ม ดังนี้ (1) เป็นเจ้าหน้าที่ผู้ดูแลระบบ ได้แก่ นักวิชาการคอมพิวเตอร์ หรือพนักงานคอมพิวเตอร์ ประจำหน่วยงานศาลในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 (2) เป็นเจ้าหน้าที่ผู้ปฏิบัติงาน ได้แก่ ข้าราชการ พนักงานราชการ และลูกจ้างชั่วคราว ประจำหน่วยงานศาลในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 (3) เป็นผู้ปฏิบัติงานไม่น้อยกว่า 1 ปี (4) เป็นผู้มีอายุไม่น้อยกว่า 25 ปี ตรวจสอบความถูกของข้อมูลด้วยเทคนิคสามเส้า จากนั้นวิเคราะห์ข้อมูลด้วยกระบวนการวิเคราะห์เนื้อหา (Content Analysis)

สรุปผลการวิจัย

ผลการศึกษาประกอบด้วยประเด็นต่างๆ ดังนี้

1. ปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 แบ่งเป็น 5 ประเภท (1) การใช้โปรแกรมประยุกต์ที่ถูกดาวน์โหลด (2) การใช้เครือข่ายไร้สาย (3) สภาพแวดล้อม ระบบไฟฟ้าขัดข้อง (4) การโจมตีแบบไม่ตั้งใจ ได้แก่ การเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งานและบุคคลอื่น ขาดแคลนบุคลากรผู้ปฏิบัติงานด้านไซเบอร์ การนำเอาอุปกรณ์อื่นมาเชื่อมต่อระบบคอมพิวเตอร์ การตั้งรหัสผ่านและการเก็บรักษารหัสผ่านระบบ การเข้าลิงค์จากอีเมล และการเข้าเว็บไซต์คอมพิวเตอร์สำหรับใช้ปฏิบัติงานไม่เพียงพอ คอมพิวเตอร์บริการคู่ความเชื่อมไปยังเครื่องคอมพิวเตอร์แม่ข่าย (5) การโจมตีแบบตั้งใจ จากการให้สัมภาษณ์ดังนี้

“...มีการดาวน์โหลดไดร์เวอร์อุปกรณ์ที่ต้องติดตั้งโปรแกรมที่อาจจะมีโฆษณา หรือลิงค์เด้งขึ้นมาซึ่งอาจแฝงภัยมาด้วย...”

(ผู้ให้ข้อมูลหลักคนที่ 8, 28 ธันวาคม 2565 : สัมภาษณ์)

“...ระบบไฟฟ้าขัดข้อง ไฟกระชาก ส่งผลทำให้อุปกรณ์ไฟล์วอลและคอมพิวเตอร์ชำรุด ทำให้เกิดช่องโหว่และข้อมูลไม่ถูกต้อง...”

(ผู้ให้ข้อมูลหลักคนที่ 35, 11 กุมภาพันธ์ 2566 : สัมภาษณ์

“...การใช้งานอุปกรณ์สื่อสารส่วนตัวที่ใช้อินเตอร์เน็ต เช่นโทรศัพท์มือถือหรือ เครื่องคอมพิวเตอร์โน๊ตบุ๊คของเจ้าหน้าที่ที่นำมาใช้งานอื่นเชื่อมต่อเครือข่ายไร้สายและใช้งานในระบบเครือข่ายภายใน...”

(ผู้ให้ข้อมูลหลักคนที่ 21, 13 มกราคม 2566 : สัมภาษณ์)

“...ผู้ใช้ล็อคอินแล้วไม่ได้ล็อคเอาท์ ทำให้เข้าถึงข้อมูลของบุคคลอื่นได้ ทำให้ คนอื่นได้รับความเสียหายได้ ล่วงรู้ข้อมูลในคดี หรือการที่มาเปิดข้อมูลแล้วไม่ปิด...”

(ผู้ให้ข้อมูลหลักคนที่ 18, 10 มกราคม 2566 : สัมภาษณ์)

“...ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี...”

(ผู้ให้ข้อมูลหลักคนที่ 2, 20 ธันวาคม 2565 : สัมภาษณ์)

สามารถสรุปได้ดังภาพที่ 1

ภาพที่ 1 ปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

2. ความสำเร็จและปัญหาอุปสรรคในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 โดยความสำเร็จ ได้แก่ (1) การรักษาความลับระบบของศาลยุติธรรมมีการกำหนดสิทธิ์ในการจัดการกับข้อมูล และอยู่ในระบบเครือข่ายภายใน ทำให้มีความปลอดภัย (2) การรักษาความถูกต้อง หัวหน้าส่วนเป็นผู้ตรวจสอบความถูกต้องของข้อมูลอีกชั้นนึง โดยข้อมูลจะถูกส่งต่อเข้าระบบที่สำนักงานอธิบดีผู้พิพากษาภาค 9 หรือสำนักงานศาลยุติธรรมตรวจสอบอีกครั้ง (3) สภาพพร้อมใช้งาน มีความพร้อมใช้งานทั้งฮาร์ดแวร์และซอฟต์แวร์ เนื่องจากอุปกรณ์หลักที่มีอยู่ในระบบจะมีเครื่องสำรองไฟฟ้าจ่ายไฟให้ทำให้ระบบทำให้มีความพร้อมใช้งาน จากการให้สัมภาษณ์ดังนี้

“...มีจำกัดในการเรียกดูตามสิทธิ์การใช้งาน หัวหน้าส่วนกำหนดสิทธิ์ของเค้าขึ้นมาเองได้...”

(ผู้ให้ข้อมูลหลักคนที่ 11, 3 มกราคม 2566 : สัมภาษณ์)

“...หัวหน้าส่วนเป็นผู้ตรวจสอบความถูกต้องของข้อมูล คนแก้ไขได้หัวหน้าส่วน การยกเลิกใบเสร็จ สิทธิ์ของหัวหน้าส่วน...”

(ผู้ให้ข้อมูลหลักคนที่ 19, 12 มกราคม 2565 : สัมภาษณ์)

“...ระบบไม่ค่อยมีปัญหา แต่แก้ไขได้ มีความพร้อมใช้งาน ทั้งฮาร์ดแวร์และซอฟต์แวร์ไม่ค่อยมีปัญหา...”

(ผู้ให้ข้อมูลหลักคนที่ 15, 9 มกราคม 2566 : สัมภาษณ์)

ส่วนปัญหาและอุปสรรค ได้แก่ (1) ด้านงบประมาณ การจัดสรรงบประมาณของโครงการต่างๆ ให้ศาลจัดซื้อเองทำให้ศาลไม่สามารถจัดซื้อได้เนื่องจากงบประมาณที่จัดสรรมาให้เป็นการประมาณราคาจากจำนวนซื้อที่มาก และมีการใช้งานระบบต่างๆ เพิ่มมากขึ้น ส่งผลให้เครื่องคอมพิวเตอร์ไม่เพียงพอในการใช้งาน และนำเครื่องที่ถูกทดแทนแล้วมาใช้งาน (2) ด้านทักษะบุคลากร ต้องมีการอบรมแนะนำเพื่อเน้นย้ำเพราะบางปัญหาบุคลากรสามารถที่จะแก้ปัญหาเบื้องต้นได้ (3) จำนวนบุคลากรทางด้านไซเบอร์ มีจำนวนไม่เพียงพอ ส่งผลให้การแก้ไขปัญหาล่าช้า ทั้งฮาร์ดแวร์และซอฟต์แวร์ และอาจทำให้เกิดความเสียหายทางด้านข้อมูลหรืออุปกรณ์ (4) ด้านนโยบายของหน่วยงาน ที่ตั้งของหน่วยงานศาลยุติธรรมอยู่ในพื้นที่ใกล้ทะเล ทำให้อุปกรณ์ต่างๆ เสื่อมสภาพชำรุดจากเกลือ และระบบที่ขึ้นมาใหม่ทำให้ผู้ใช้งานระบบจะต้องเรียนรู้ระบบใหม่ๆอยู่ตลอดเวลาทำผู้ใช้งานมีรหัสที่ต้องจำรหัสมากขึ้น มีระบบเพิ่มมาใหม่ มีงานที่ซ้ำซ้อนอยู่ จากการให้สัมภาษณ์ดังนี้

“...ด้านงบประมาณ ของโครงการของบประมาณต่างๆ จัดสรรเอามาให้ศาลจัดซื้อเองทำให้ศาลไม่สามารถจัดซื้อเองได้ในงบประมาณที่จัดสรรมาให้เพราะงบดังกล่าวอยู่ในราคาที่จัดซื้อได้ในจำนวนที่ซื้อหลายเครื่อง...”

(ผู้ให้ข้อมูลหลักคนที่ 11, 3 มกราคม 2566 : สัมภาษณ์)

“...ด้านทักษะบุคลากร มีปัญหาเล็กน้อย ขาดทักษะการใช้งานคอมพิวเตอร์ ต้องเน้นย้ำการใช้งานและทบทวน...”

(ผู้ให้ข้อมูลหลักคนที่ 10, 29 ธันวาคม 2565 : สัมภาษณ์)

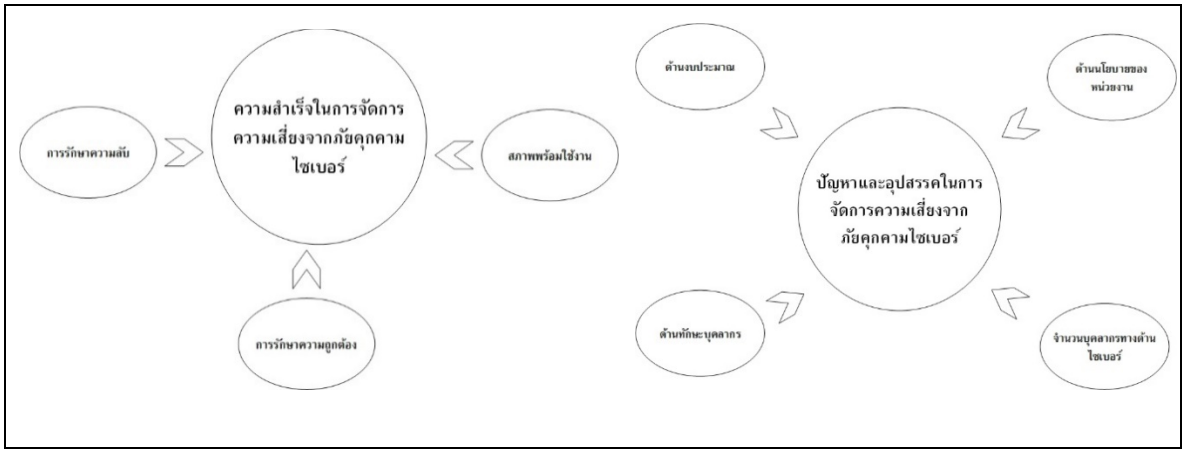
“...ให้มีเจ้าหน้าที่ด้านคอมพิวเตอร์เพิ่มขึ้นในศาลที่ปริมาณคอมพิวเตอร์จำนวนมากหรือศาลที่มีงานคดีหรือผู้ใช้บริการจำนวนมาก เพื่อส่งเสริมงานและลดความเสี่ยงจากความเสี่ยงจากภัยคุกคามไซเบอร์...”

(ผู้ให้ข้อมูลหลักคนที่ 21, 13 มกราคม 2566 : สัมภาษณ์)

“...ศาลอยู่ใกล้ทะเล เกลือ ทำให้ Core Switch พัดลมพัง ใช้งานเน็ตไม่ได้ Server พัง ไอน้ำ ขี้เกลือ สนิม...”

(ผู้ให้ข้อมูลหลักคนที่ 9, 29 ธันวาคม 2565 : สัมภาษณ์)

สามารถสรุปได้ดังภาพที่ 2



ภาพที่ 2 ความสำเร็จและปัญหาอุปสรรคในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9

การอภิปรายผล

จากการศึกษาเรื่องการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ : บทเรียนของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 อภิปรายผลได้ดังนี้

1. ปัจจัยความเสี่ยงจากการใช้โปรแกรมประยุกต์ที่ถูกดาวน์โหลด เช่น ติดตั้งไดร์เวอร์เพื่อติดตั้งอุปกรณ์ หรือการดาวน์โหลดโปรแกรมสำหรับการใช้งานโปรแกรมต่างๆ ที่เจ้าหน้าที่ต้องการจะติดตั้งเพื่อใช้งานโดยโปรแกรมต่างๆ ซึ่งอาจอยู่ในรูปแบบฟรีแวร์ แชร์แวร์ โปรแกรมดังกล่าวมีความเสี่ยงที่จะนำพาไวรัสหรือ สิ่งไม่พึงประสงค์เข้ามาในระบบคอมพิวเตอร์ได้ การใช้เครือข่ายไร้สายที่เกิดความเสี่ยงจากการที่นำเอาอุปกรณ์ส่วนตัว ได้แก่ โทรศัพท์มือถือ เครื่องคอมพิวเตอร์แบบพกพา ซึ่งอาจมีไวรัสหรือสิ่งไม่พึงประสงค์แปลกปลอมเข้ามาด้วยผ่านการเชื่อมต่อเครือข่ายไร้สายภายในศาลได้ โดยปัจจัยความเสี่ยงจากภัยคุกคามไซเบอร์ข้างต้น สอดคล้องกับ วิศณุ สร้างวงศ์ใหม่ (2561) ศึกษาการเป็นมืออาชีพในการรักษาความปลอดภัยไซเบอร์ และณรงค์เวตย์ เรืองจวง (2561) ศึกษาแนวทางการพัฒนาขีดความสามารถบุคลากรด้านไซเบอร์ของกองทัพอากาศ ปัจจัยการโจมตีแบบตั้งใจเป็นกรณีที่ระบบอาจมีโอกาสที่จะถูกโจมตีแบบตั้งใจจากผู้ไม่ประสงค์ดีได้หลากหลายช่องทาง หรือจากการขาดความรู้ความตระหนักของเจ้าหน้าที่ผู้ปฏิบัติงานหรือผู้ดูแลระบบก็เป็นช่องโหว่ที่ทำให้ผู้ไม่ประสงค์ดีเข้ามาในระบบได้โดยง่าย ปัจจัยการโจมตีแบบไม่ตั้งใจสามารถแยกออกเป็นหลายประเด็น ได้แก่ การเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งานและบุคคลอื่น การขาดแคลนบุคลากรด้านไซเบอร์ การนำเอาอุปกรณ์อื่นมาเชื่อมต่อระบบคอมพิวเตอร์ การตั้งรหัสผ่านและการเก็บรักษารหัสผ่านการเข้าลิงค์จากอีเมล และการเข้าเว็บไซต์ คอมพิวเตอร์สำหรับใช้ปฏิบัติงานไม่เพียงพอ คอมพิวเตอร์บริการคู่ความเชื่อมไปยังเครื่องคอมพิวเตอร์แม่ข่าย การติดตั้งโปรแกรมแอนตี้ไวรัสบางเครื่องไม่สามารถทำได้ จากผลการศึกษาในประเด็นนี้เป็นปัจจัยการโจมตีที่มีความสำคัญมากที่สุด เนื่องจาก

เกี่ยวกับความรู้ทักษะความตระหนักรู้ของผู้ปฏิบัติงานและผู้ดูแลระบบ เป็นช่องโหว่ที่ทำให้เกิดความเสี่ยงจากภัยคุกคามไซเบอร์ในด้านนี้มาก ด้านปัจจัยความเสี่ยงจากการภัยคุกคามไซเบอร์จากสภาพแวดล้อมที่เกิดจากระบบไฟฟ้าขัดข้อง ได้แก่ ไฟตก ไฟกระชาก ซึ่งจะส่งผลต่อฮาร์ดแวร์และซอฟต์แวร์ ซึ่งสอดคล้องกับ อนาวิล แก้วสะอาด และ ณัฐวี อุตกฤษฎ์ (2564) ศึกษาเรื่องการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร

2. ความสำเร็จในการจัดการความเสี่ยงจากภัยคุกคามไซเบอร์ของหน่วยงานศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 มี 3 ด้าน ได้แก่ (1) ด้านการรักษาความลับของหน่วยงานศาลยุติธรรม ระบบต่างๆ ของสำนักงานศาลยุติธรรมจะมีการกำหนดสิทธิในการเข้าถึงข้อมูลในการปฏิบัติหน้าที่ตามอำนาจหน้าที่ (2) ด้านการรักษาความถูกต้อง ข้อมูลในระบบของฐานข้อมูล มีความถูกต้อง ครบถ้วนแม่นยำ เนื่องจากมีการตรวจข้อมูลก่อนส่งข้อมูลรายงานไปที่สำนักศาลยุติธรรมประจำภาค 9 สำนักแผนงานและงบประมาณ และสำนักส่งเสริมงานตุลาการ (3) สภาพพร้อมใช้งาน ความพร้อมใช้งานของฮาร์ดแวร์ขึ้นอยู่กับระบบไฟฟ้าถ้าอุปกรณ์มีเครื่องสำรองไฟฟ้าจะทำให้อุปกรณ์ดังกล่าว ลดการเสื่อมสภาพของอุปกรณ์ มีความพร้อมใช้งาน

ส่วนปัญหาและอุปสรรค ด้านงบประมาณในการจัดซื้อทั้งฮาร์ดแวร์และซอฟต์แวร์ ต้องรองบประมาณสนับสนุน ไม่สามารถจัดซื้อได้เนื่องด้วยราคาที่สูง คอมพิวเตอร์ที่มีไม่เพียงพอเนื่องจากระบบงานต่างๆ เพิ่มขึ้น โปรแกรมที่จำเป็นและไม่มีลิขสิทธิ์ เสนอแนะให้ส่วนกลางเป็นผู้จัดซื้อและจัดส่งครุภัณฑ์คอมพิวเตอร์มาให้ตามศาลต่างๆ เสนอสำนักเทคโนโลยีสารสนเทศ สำรวจความต้องการเพิ่มเติมครุภัณฑ์คอมพิวเตอร์ที่ยังไม่เพียงพอ และตามจุดต่างๆ ตามความจำเป็น ความต้องการใช้โปรแกรมที่มีความจำเป็นต้องใช้งานแต่ไม่มีลิขสิทธิ์ และอุปกรณ์เครือข่ายที่หมดอายุการรับประกันเพื่อต่อประกันและบำรุงรักษาอุปกรณ์เครือข่ายอยู่เสมอ เสนอของบประมาณไปที่สำนักศาลยุติธรรมประจำภาค 9 เพื่อของบต่อที่สำนักแผนงานและงบประมาณ ด้านทักษะบุคลากร การนำระบบต่างๆ มาใช้ในการสนับสนุนการปฏิบัติงาน ปัจจุบันภัยคุกคามไซเบอร์มีหลากหลายช่องทางหลากหลายรูปแบบ

ข้อเสนอแนะได้แก่ กรณีระบบมีความคล้ายคลึงเหมือนกันควรปรับเป็นโปรแกรมเดียวกัน ผู้ใช้งานระบบจะได้สะดวกในการปฏิบัติงาน การอบรมหรือพัฒนาทักษะให้กับเจ้าหน้าที่ผู้ปฏิบัติงานและเจ้าหน้าที่ผู้ดูแลระบบศาลยุติธรรมในเขตอำนาจอธิบดีผู้พิพากษาภาค 9 ต้องทบทวนให้สม่ำเสมอ ด้านจำนวนบุคลากรทางด้านไซเบอร์ ขาดแคลนไม่สามารถรองรับการปฏิบัติงานในการแก้ไขปัญหาได้ทันท่วงที ควรขออัตรากำลังเพิ่มเติม ตามขนาดศาลหรือปริมาณคดี หรือคอมพิวเตอร์ หรือผู้รับบริการ โดยจัดทำข้อมูลประกอบให้กับสำนักงานศาลยุติธรรม หรือการใช้บุคลากรทางด้านไซเบอร์ร่วมกันภายในจังหวัด และอาจขอเจ้าหน้าที่ผู้ดูแลระบบของสำนักศาลยุติธรรมประจำภาค 9 ไปช่วยดูแลระบบซึ่งเกิดปัญหาต้องรีบแก้ไข หรือ

อาจแต่งตั้งเจ้าหน้าที่ผู้ปฏิบัติงานด้านดิจิตอลเพิ่มเติม ด้านนโยบายของหน่วยงาน การตั้งอาคารที่ทำการอยู่ใกล้ทะเลควรออกแบบอาคารและวัสดุในการปกป้องอุปกรณ์ ครุภัณฑ์ต่างๆ ไม่ให้เกิดความเสียหาย ไม่ให้เกิดคราบเกลือ สนิม และระบบใหม่ควรเป็นระบบที่ไม่ซ้ำซ้อนกับระบบเดิมที่มีอยู่เดิม

เอกสารอ้างอิง

กมลพร บุญนนทารมย์ และศันสนีย์ จะสุวรรณ. (2564). การบริหารความเสี่ยงอย่างมืออาชีพ. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก http://www.journalgrad.ssru.ac.th/index.php/8thconference/article/view/2523.

กริน ธัญญวิกร และธีระ กุลสวัสดิ์. (2564). การจัดการความมั่นคงทางเทคโนโลยีสารสนเทศ กรณีศึกษาการคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so04.tci-thaijo.org/index.php/JSBA/article/view/247389/169638.

เกียรติศักดิ์ ลุยทอง. (2561) การพัฒนาระบบตรวจสอบ เฝ้าระวัง และแจ้งเตือนการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์ไซเบอร์กองทัพบก. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก http://dspace.spu.ac.th/bitstream/123456789/5747/2/OK_%e0%b8%a3%e0%b8%a7%e0%b8%a1%e0%b9%80%e0%b8%a5%e0%b9%88%e0%b8%a1%e0%b8%aa%e0%b8%a1%e0%b8%9a%e0%b8%b9%e0%b8%a3%e0%b8%93%e0%b9%8c.pdf

คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย. (2563). ประกาศคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เรื่องหลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกันวินาศภัย พ.ศ. 2563. สืบค้นเมื่อ 1 มิถุนายน 2565, จากhttps://www.tgia.org/upload/file_group/16/download_1883.pdf.

ชฎาภรณ์ สิงห์แก้ว. (2564). บทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so06.tci-thaijo.org/index.php/umt-poly/article/view/249037/168688.

ญาณิศา เผื่อนเพาะ. (2562). การจัดการความเสี่ยงในธุรกิจขนาดกลางและขนาดย่อม. สืบค้นเมื่อ 1 มิถุนายน 2565, http://msjournals.aru.ac.th/index.php/msjournals/article/view/90/21.

ณรงค์เวตย์ เรืองจวง. (2561). แนวทางการพัฒนาขีดความสามารถบุคลากร ด้านไซเบอร์ของกองทัพอากาศ. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so05.tci-thaijo.org/index.php/ratthapirak/article/view/189480/132695.

ธนภัทร กิตติวณิชพันธุ์ และอานนท์ ทับเที่ยง. (2561). สมรรถนะของบุคลากรในหน่วยงานราชการด้านความมั่นคงปลอดภัยไซเบอร์ตามข้อกำหนด NIST และมาตรฐาน ISO27001/2013. สืบค้นเมื่อ

1 มิถุนายน 2565, จาก https://ph02.tci-thaijo.org/index.php/ET/article/view/243980/165443.

ธีระศักดิ์ เปี่ยมสุภัคพงศ์, ธีระรัตน์ เปี่ยมสุภัคพงศ์, พรพรรณ สุวรรณประทีป, สุกานดา โรจนประภายนต์ และวัฒนา เสรีคุณากุล. (2561-2562). การเรียนรู้เพื่อรับมือกับการบริหารความเสี่ยงของธุรกิจในบริบทใหม่ ยุคอุตสาหกรรม 4.0. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so03.tci-thaijo.org/index.php/trujournal/article/view/193524/148978.

นริส อุไรพันธ์ และธรนี มณีศรี. (2563). โมเดลสมการเชิงโครงสร้าง เพื่อวิเคราะห์ปัจจัยที่ส่งผลต่อการคืนสภาพได้ทางไซเบอร์ของดิจิทัลซัพพลายเชน สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก http://dspace.spu.ac.th/bitstream 123456789/6701/1/%e0%b8%9a%e0%b8%97%e0%b8%84%e0%b8%a7%e0%b8%b2%e0%b8%a1%e0%b8%a7%e0%b8%b4%e0%b8%88%e0%b8%b1%e0%b8%a2%201.pdf.

ปรัชญา เฉลิมวัฒน์. (2560). แนวทางการพัฒนากำลังพลด้านไซเบอร์เพื่อพร้อมรับภัยคุกคามระดับชาติ. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก http://www.dsdw2016.dsdw.go.th/doc_pr/ndc_2560-2561/PDF/8451sc/%E0%B8%A3%E0%B8%A7%E0%B8%A1.pdf.

ฝ่ายวิเคราะห์เทคโนโลยีป้องกันประเทศ. (2559). ภัยคุกคามทางไซเบอร์ (Cyber Security). สืบค้นเมื่อ 1 มิถุนายน 2565, จาก http://dtd.dti.or.th/jspui/bitstream/123456789/1880/1/%e0%b8%a0%e0%b8%b1%e0%b8%a2%e0%b8%84%e0%b8%b8%e0%b8%81%e0%b8%84%e0%b8%b2%e0%b8%a1%e0%b8%97%e0%b8%b2%e0%b8%87%e0%b9%84%e0%b8%8b%e0%b9%80%e0%b8%9a%e0%b8%ad%e0%b8%a3%e0%b9%8c%20%28Cyber%20Security%29.pdf.

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (24 พฤษภาคม 2562). *ราชกิจจานุเบกษา.* เล่ม 136 ตอนที่ 69 ก หน้า 20-51. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF.

พิชญาพร พีรพันธุ์ และวิโรจน์ เจษฎาลักษณ์. (2564). กรอบแนวคิดปัจจัยเชิงสาเหตุและผลลัพธ์ของความสามารถในการจัดการความเสี่ยงขององค์กร. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so03.tci-thaijo.org/index.php/trujournal/article/view/249409/170470.

เมธาพร ธรรมศิริ และศิรภัสสศ์ วงศ์ทองดี. (2565). ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so05.tci-thaijo.org/index.php/TRDMJOPOlSU/article/view/259170/174347.

ยุทธศักดิ์ รักเสรีพิทักษ์ และศิริลักษม์ ตันตยกุล. (2565). บทบาทของกองทัพกับนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันภัยคุกคามรูปแบบใหม่. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก http://202.41.160.104/index.php/MPA/article/view/316/258.

วิลาส วิถีไพร. (2561). การพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง. สืบค้นเมื่อเมื่อ 1 มิถุนายน 2565, จาก http://www.dspace.spu.ac.th/bitstream/123456789/5769/1/IS_All_Wilas_Sep%2017%2c%202018.pdf.

วิจิตรา สีแดงกล่ำ. (2562). การบริหารความเสี่ยงขององค์กรในศตวรรษที่ 21. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก http://journalgrad.ssru.ac.th/index.php/miniconference/article/view/2050.

วิศณุ สร้างวงศ์ใหม่. (2561). การเป็นมืออาชีพในการรักษาความปลอดภัยไซเบอร์. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so05.tci-thaijo.org/index.php/ratthapirak/article/view/188754/132306.

สุฏิกา รักประสูติ. (2558). บทบาทของผู้ตรวจสอบภายในต่อการจัดการความเสี่ยงองค์กร: ปัจจัยสาเหตุและผลลัพธ์. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so05.tci-thaijo.org/index.php/DPUSuthiparithatJournal/article/view/ 244357/166034.

สุภาพร พรมโส, ปราลี มณีรัตน์ และประสงค์ ปราณีตพลกรัง. (2564). สถานภาพความพร้อมและดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของมหาวิทยาลัยราชภัฏ สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://ph02.tci-thaijo.org/index.php/nkrafa-sct/article/view/244698/166774.

สุวันต์นา เสมอเนตร. (2561). การพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ภายใต้มาตรฐาน ISO/IEC 27001:2013 ศูนย์ปฏิบัติการ Ministry of Public Health Data Center (MOPH IDC). สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://thaidj.org/index.php/JHS/article/view/5914/5747.

อนาวิล แก้วสะอาด และณัฐวี อุตกฤษฎ์. (2564). แนวทางบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so04.tci-thaijo.org/index.php/ndsijournal/article/view/245941/170493.

อรรคเดช ประทีปอุษานนท์ และธาราทิพย์ กัลยาณมิตร. (2560). แนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ วารสารสถาบันวิชาการป้องกันประเทศ. สืบค้นเมื่อ 1 มิถุนายน 2565, จาก https://so04.tci-thaijo.org/index.php/ndsijournal/article/view/107618/85175.