การวิเคราะห์การรักษาความมั่นคงทางไซเบอร์ของธนาคารพาณิชย์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

Analysis of Cyber Security for Commercial Banks in Compliance with the Cyber Security Act 2019

สุรพงศ์ ทรัพยาคม* และ อรรถพล ป้อมสถิตย์

Surapong Sappayakhom* and Auttapon Pomsathit

วิทยาลัยนวัตกรรมดิจิทัลและเทคโนโลยีสารสนเทศ มหาวิทยาลัยรังสิต ปทุมธานี ประเทศไทย

College of Digital Innovation and Information Technology (DIIT), Rangsit University, Pathum Thani, Thailand

**Corresponding author, E-mail: surapong.s58@rsu.ac.th*

บทคัดย่อ

การรักษาความมั่นคงทางไซเบอร์ของธนาคารพาณิชย์มีความจำเป็นและส่งผลกระทบโดยตรงต่อการให้บริการ อีกทั้งปัจจุบันพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 คือมาตรการหรือการดำเนินการที่กำหนดขึ้นเป็นกรอบเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อเศรษฐกิจและความมั่นคงของประเทศ จึงเป็นภารกิจใหม่และมีมาตรฐานที่ซับซ้อนที่ไม่เคยปฏิบัติมาก่อน และมาตรการดังกล่าวส่งผลกระทบในวงกว้างต่อผู้ให้บริการ และผู้รับบริการของธนาคารพาณิชย์ไทยซึ่งมีการวิเคราะห์การดำเนินการรักษาความมั่นคงทางไซเบอร์ดังนี้ 1) ด้านเทคนิค อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย เครื่องมือ และอุปกรณ์ อาจเกิดถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดีหรือถูกก่อกวนจากผู้ประสงค์ร้าย ถูกเจาะทำลายระบบ 2) ด้านผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่าง ๆ ของธนาคารพาณิชย์เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้ 3) ด้านภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม หรือความไม่สงบเรียบร้อยในบ้านเมือง 4) ด้านการบริหารจัดการ เป็นความเสี่ยงจากการวางแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการรักษาความมั่นคงทางไซเบอร์ และ 5) เสนอแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงทางไซเบอร์ที่เหมาะสมและสอดคล้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์แบ่งออกเป็น 5 ฟังก์ชันหลัก คือ 1) การระบุและเข้าใจถึงบริบทต่าง ๆ เพื่อการบริหารจัดการความเสี่ยง 2) การวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กร 3) การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อตรวจจับสถานการณ์

เอกสารสืบเนื่องจากการประชุมวิชาการระดับชาติ มหาวิทยาลัยรังสิต ประจำปี 2563

ที่ผิดปกติ 4) การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น และ 5) การกำหนดขั้นตอนและกระบวนการต่าง ๆ เพื่อให้สามารถดำเนินได้อย่างต่อเนื่อง และฟื้นฟูระบบให้กลับคืนมาเหมือนเดิม

คำสำคัญ: *ด้านความมั่นคงทางไซเบอร์ กรอบการทำงาน การระบุตัวตน การป้องกัน การตรวจจับ การตอบสนอง การกู้คืน*

Abstract

Cybersecurity Act 2019 is main standard to prevent, protect, and reduce risks from cyber threats from inside and outside country that has significant impacts to economic and national security. Commercial banks need to implement cybersecurity policy & guidelines following this act due to its significant impacts on both customers and themselves as service providers. Thai commercial banks were found to implement Cybersecurity measure including: 1) technical risks caused by computer system, network, devices, malwares, hackers, or cybercriminals; 2) IT operation staff accessing to inappropriate data or using commercial bank's confidential information without authority; 3) unexpected incidents including risks caused by natural disasters or high-risk incidents: electrical interruption, flood, fire, or political chaos; and 4) Management policy with impacts on cybersecurity operation. This study recommended commercial banks to implement cybersecurity protection measures according to NIST Cybersecurity framework as follows: 1) identification and understanding of contexts for risk management, 2) implementation of standards for the protection of the organization's system, 3) self-preparation for unexpected incidents, 4) risk management planning for unexpected incidents, and 5) planning for business continuity management and recovery.

Keywords: *Cyber Security, Framework, Identification, Protection, Detection, Response, Retreival,*

1. บทนำ

การโจมตีทางไซเบอร์ในปัจจุบันเป็นไปอย่างกว้างขวางมีตั้งแต่การลักขโมยข้อมูลไปจนถึงการก่อการร้ายระดับประเทศด้านไซเบอร์ หน่วยงานหรือองค์กรที่ถูกโจมตีมีหลากหลายด้าน ทั้งด้านการเงินการธนาคาร ด้านพลังงาน ด้านการแพทย์ และด้านการทหาร เป็นต้น ปัญหาการโจมตีทางไซเบอร์เป็นปัญหาในระดับประเทศที่เกี่ยวข้องทั้งภาครัฐและภาคเอกชนหน่วยงานและองค์กรต่าง ๆ ที่ส่งผลกระทบทางเศรษฐกิจและสังคมอย่างมาก ซึ่งรัฐบาลได้เห็นความสำคัญของการรักษาความมั่นคงทางไซเบอร์ จึงได้ผลักดันจนสามารถประกาศใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ในเดือนพฤษภาคม ปี 2562 (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, 2562) โดยจะกำหนดแนวทางในการจัดการ การป้องกัน การรับมือ และการลดความเสี่ยงทางไซเบอร์ มีการประสานความร่วมมือระหว่างผู้เกี่ยวข้อง พัฒนาความรู้ความสามารถของบุคลากรและผู้เชี่ยวชาญ รวมถึงการให้ความรู้และความตระหนักถึงภัยไซเบอร์อีกด้วย

ธนาคารพาณิชย์ซึ่งมีภารกิจเกี่ยวกับการมุ่งสู่ความเป็นสถาบันการเงินชั้นนำระดับภูมิภาคที่ก้าวสู่เวทีโลกด้วยการเติบโตที่ยั่งยืน รับผิดชอบต่อสังคม และสนองต่อความต้องการของลูกค้า แต่เนื่องจากการกำหนดมาตรการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นภารกิจใหม่และมีมาตรฐานที่ซับซ้อนที่ไม่เคยปฏิบัติมาก่อน และมาตรการดังกล่าวส่งผลกระทบในวงกว้างต่อผู้ให้บริการและผู้รับบริการของธนาคารพาณิชย์ทั่วประเทศ ดังนั้นจึงมีความจำเป็นที่ต้องประเมินสถานการณ์และมาตรการที่ธนาคารพาณิชย์ปฏิบัติอยู่ เพื่อให้เป็นแนวทางในการจัดทำนโยบายและแนวปฏิบัติ

ในการรักษาความมั่นคงทางไซเบอร์ของธนาคารพาณิชย์มีความเหมาะสมสอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และเป็นการเตรียมความพร้อมในการหามาตรการที่เหมาะสมสอดคล้องตามกฎหมายลูกพระราชบัญญัติที่จะประกาศใช้กับหน่วยงานของรัฐและเอกชนทั่วประเทศต่อไป

การใช้เทคโนโลยีสนับสนุนการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีหลายแบบได้แก่ การใช้แอคทีฟไดเรคทอรี่ (Active Directory) ในการทำระบบการยืนยันตัวบุคคลอย่างบูรณาการ (Single Sign-On) เพื่อให้องค์กรมีความสามารถในการบริหารจัดการใช้งานทรัพยากรด้านสารสนเทศได้อย่างบูรณาการ จากการที่จะกำหนดการเข้าใช้งานระบบต่าง ๆ ให้เป็นไปตามสิทธิ์ของบัญชีผู้ใช้งานได้เป็นอันหนึ่งอันเดียวกันแม้ว่าระบบหรืออุปกรณ์ต่าง ๆ (พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562, 2562) จะถูกสร้างหรือพัฒนาจากผู้ผลิตที่แตกต่างกันก็ตาม และระบบไฮเปอร์คอนเวอจ์อินฟราสตรัคเจอร์ (Hyper Converged Infrastructure) (Sverdlik, 2015) ที่เป็นเทคโนโลยีในการควบรวมโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ ทั้งเครือแม่ข่าย การจัดเก็บข้อมูลและระบบโครงข่ายไว้ในระบบเดียวให้ทำงานได้ต่อเนื่อง มีปัญหาน้อยลง หากระบบใดมีปัญหาแล้วระบบอื่นจะสามารถทำงานแทนได้ ดังนั้นในการพัฒนาระบบบริหารจัดการคลังข้อมูลกลางด้านข้อมูลส่วนบุคคลเพื่อการให้บริการประชาชนด้วยระบบต่าง ๆ ที่กล่าวไว้ข้างต้นจะทำให้ผู้ใช้บริการของธนาคารมีความสะดวก รวดเร็ว และปลอดภัยยิ่งขึ้น

2. วัตถุประสงค์

1. เสนอแนะแนวทางการป้องกันภัยคุกคามให้สอดคล้องกับตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

2. วิเคราะห์ความเสี่ยงในการรักษาความมั่นคงทางไซเบอร์ของธนาคารพาณิชย์

3. วิธีดำเนินการวิจัย

ในการเก็บข้อมูลความมั่นคงทางไซเบอร์ของธนาคารพาณิชย์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ของธนาคารพาณิชย์มีการดำเนินการเก็บข้อมูลโดยมีขั้นตอนในการทำดังนี้

3.1 กลุ่มตัวอย่าง

กลุ่มตัวอย่างที่ใช้ คือ

1. ผู้บริหารฝ่ายพัฒนาระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ

2. เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ฝ่ายบริการผู้ใช้งานระบบเทคโนโลยีสารสนเทศ เจ้าหน้าที่ปฏิบัติการคอมพิวเตอร์ฝ่ายระบบโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ

3.2 เครื่องมือที่ใช้ในการเก็บข้อมูล

เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลนั้นได้สร้างแบบสอบถาม และประมวลจากเอกสารงานวิจัยที่เกี่ยวข้อง จากนั้นสร้างแบบสัมภาษณ์ขึ้นให้ครอบคลุมกับวัตถุประสงค์การวิจัย แล้วจึงนำแบบสอบถาม และสัมภาษณ์ไปเก็บข้อมูลจากบุคลากรที่ปฏิบัติงานด้านระบบสารสนเทศ ทั้งในระดับบริหาร และระดับปฏิบัติงานดังนี้

3.2.1 แบบสอบถาม แบ่งออกเป็น 3 ส่วน

ส่วนที่ 1 ข้อมูลเกี่ยวกับการรักษาความมั่นคงทางไซเบอร์ของธนาคาร

ส่วนที่ 2 การพัฒนาศักยภาพบุคลากรด้านการรักษาความมั่นคงทางไซเบอร์ของธนาคาร

ส่วนที่ 3 ข้อเสนอแนะ

3.2.2 แบบสัมภาษณ์ การรักษาความมั่นคงทางไซเบอร์ของธนาคารพาณิชย์

3.3 วิเคราะห์ความเสี่ยงในการรักษาความมั่นคงทางไซเบอร์ของธนาคารพาณิชย์

3.3.1 การประเมินค่าความเสี่ยง (Risk evaluation)

การประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยจากขั้นตอนที่ผ่านมาจากแบบสัมภาษณ์และแบบสอบถาม ได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ ซึ่งการวัดระดับความเสี่ยงมีการกำหนดแผนภูมิความเสี่ยงที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยงโดยสามารถคำนวณระดับความเสี่ยงได้คือ ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ x ผลกระทบ

ซึ่งใช้เกณฑ์ในการจัดแบ่งได้ดังตารางที่ 1 ดังนี้

ตารางที่ 1 เกณฑ์ในการจัดแบ่งการประเมินค่าความเสี่ยง

ระดับความเสี่ยง	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
1 – 8	ต่ำ	ยอมรับความเสี่ยง	ขาว
9 – 16	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง
17 – 24	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	ฟ้า
25	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

4. ผลการวิจัย

ผลการวิเคราะห์แนวทางการดำเนินการรักษาความมั่นคงทางไซเบอร์ของธนาคารพาณิชย์ประกอบด้วย

4.1 ด้านเทคนิค

4.1.1 ธนาคารพาณิชย์มีการทำระบบการยืนยันตัวบุคคลอย่างบูรณาการโดยการใช้เทคโนโลยี แอคทีฟไดเรคทอรี่เพื่อความสะดวก และปลอดภัย ในการเข้าใช้งานและการบริหารจัดการสารสนเทศเพื่อจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานในการเข้าถึงทรัพยากรสารสนเทศของส่วนกลางและเครื่องส่วนบุคคลผ่านทั้งระบบเครือข่ายสาย (LAN) และ ระบบเครือข่ายไร้สาย (Wi-Fi) อีกทั้งเป็นการควบคุมผู้ใช้งานใช้งานฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชันตามสิทธิ์อันเป็นไปตามบทบาทหน้าที่และความรับผิดชอบและพบว่าธนาคารพาณิชย์ได้มีการใช้เทคโนโลยีโครงข่ายภายในเสมือน (Virtual Private Network) (อรรถพล ป้อมสถิตย์, 2561) อยู่แล้วซึ่งเป็นการควบคุมเส้นทางการสื่อสารที่มีความปลอดภัยสูงจากเชื่อมต่อส่วนกลางไปยังส่วนภูมิภาครวมถึงบุคลากรที่ได้รับอนุญาตเป็นการเฉพาะ จึงจะมีการเชื่อมต่อแอคทีฟไดเรคทอรี่เพื่อเพิ่มประสิทธิภาพในการบริหารจัดการผู้ใช้อย่างบูรณาการ

4.1.2 ธนาคารพาณิชย์มีการจัดหาซอฟต์แวร์ลิขสิทธิ์ในการรักษาความปลอดภัยเครื่องคอมพิวเตอร์ส่วนบุคคล และเครื่องคอมพิวเตอร์แม่ข่าย

4.1.3 ธนาคารพาณิชย์มีการจัดหาอุปกรณ์ในการควบคุมความปลอดภัยระบบเครือข่ายอยู่แล้วประกอบด้วย เช่น ไฟล์วอลล์ (Firewall) ระบบตรวจจับหรือป้องกันการบุกรุก (Intrusion Detection System/Intrusion Prevention System), การควบคุมการเข้าใช้งานเครือข่าย (Network Access Control)

4.1.4 ธนาคารพาณิชย์มีการดำเนินการให้บริการเครือข่ายไร้สาย แต่การรักษาความปลอดภัยในการเข้าใช้งานเป็นลักษณะเครื่องต่อเครื่อง ไม่มีสามารถดำเนินการในภาพรวม

4.1.5 ธนาคารพาณิชย์มีการดำเนินการรักษาความปลอดภัยระบบเครือข่าย แต่เป็นลักษณะเครื่องต่อเครื่องโดยต้องทำบัญชีการจัดเก็บชื่อผู้ใช้งานและรหัสผ่านแยกทีละเครื่อง และมีการทำงานแยกส่วนกันเช่น ระบบฐานข้อมูลระบบเว็บ

4.2 ด้านผู้ปฏิบัติงาน

4.2.1 ธนาคารพาณิชย์มีการมอบอำนาจหน้าที่ในการปฏิบัติตามลำดับชั้น แต่ไม่มีการกำหนดเป็นแนวนโยบายและปฏิบัติที่เป็นลายลักษณ์อักษร

4.2.2 ในส่วนของการเข้าถึงระบบสารสนเทศผ่านเครือข่ายไร้สายธนาคารพาณิชย์ได้มีการดำเนินการจัดความสำคัญในการเข้าถึงข้อมูลที่ไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยเป็นการกำหนดรหัสการเข้าใช้งานแยกเป็นส่วน ๆ ไม่มีการควบคุมแบบศูนย์กลางดังนั้นหากไม่ได้ตั้งค่าการรักษาความปลอดภัยที่เหมาะสม (อินทัช โฮลดิ้งส์ จำกัด (มหาชน), 2560) ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกอื่น ๆ ที่รับสัญญาณได้เชื่อมต่อเข้ากับระบบเครือข่ายของธนาคารพาณิชย์ทำให้เกิดช่องโหว่กับระบบรักษาความปลอดภัย

4.3 ด้านภัยหรือสถานการณ์ฉุกเฉิน

4.3.1 ธนาคารพาณิชย์มีการดำเนินการด้านการสำรองระบบฐานข้อมูลตามรอบการทำงานปกติ และการสร้างศูนย์ข้อมูลสำรอง (Disaster Recovery Site) เป็นที่เรียบร้อยแล้วนั้นหมายถึงหน่วยงานส่วนกลางสามารถแก้ไขปัญหาระบบสารสนเทศที่เกิดขึ้นจากภัยพิบัติต่างๆ นอกสถานที่ได้

4.4 ด้านการบริหารจัดการ

4.4.1 ผู้บริหารธนาคารพาณิชย์มีการดำเนินการมอบหมายให้เจ้าหน้าที่ที่เหมาะสมดำเนินการต่าง ๆ ในการดูแลระบบคอมพิวเตอร์เพื่อรักษาความมั่นคงปลอดภัยตามสายงาน

4.4.2 ธนาคารพาณิชย์มีการตรวจสอบและประเมินความเสี่ยงที่เป็นภาพรวมทั้งองค์กร

5. การอภิปรายผล

ผลการวิเคราะห์ข้อมูลเชิงคุณภาพได้สะท้อนถึงบทบาทการรักษาความมั่นคงทางไซเบอร์ของธนาคารพาณิชย์ซึ่งเข้าไปสร้างแนวทางในการปรับปรุงพัฒนาความมั่นคงทางไซเบอร์ของธนาคารพาณิชย์โดยให้พิจารณาพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกรอบทำงาน NIST Cyber security Framework (NIST, 2018) เป็นสำคัญดังนี้

5.1 ด้านเทคนิค

5.1.1 ธนาคารพาณิชย์จะมีการทำระบบการยืนยันตัวบุคคลอย่างบูรณาการ โดยการใช้แอคทีฟไดเรคทอรี่เพื่อความสะดวก และปลอดภัย ในการเข้าใช้งานและการบริหารจัดการสารสนเทศเพื่อจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานในการเข้าถึงทรัพยากรสารสนเทศของส่วนกลางและเครื่องส่วนบุคคลผ่านทั้งระบบเครือข่ายสายและระบบเครือข่ายไร้สาย อีกทั้งเป็นการควบคุมผู้ใช้งานใช้งานฟังก์ชันต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน

5.1.2 ธนาคารพาณิชย์จะมีการเชื่อมต่อแอคทีฟไดเรคทอรี่เพื่อเพิ่มประสิทธิภาพในการบริหารจัดการผู้ใช้จากจุดเดียวกับเทคโนโลยีโครงข่ายภายในเสมือน (Virtual Private Network) ในการควบคุมเส้นทางการสื่อสารที่มีความปลอดภัยสูงจากเชื่อมต่อส่วนกลางไปยังส่วนภูมิภาค

5.1.3 ธนาคารพาณิชย์จะมีการดำเนินการจัดหาซอฟต์แวร์ลิขสิทธิ์ในการรักษาความปลอดภัยอย่างต่อเนื่องเพราะซอฟต์แวร์ดังกล่าวจำเป็นจะต้องมีการอัพเดทฐานข้อมูลเพื่อความทันสมัย ในตรวจจับไวรัสหรือโปรแกรมไม่ประสงค์ดีที่มีการเปลี่ยนแปลงตลอดเวลา

5.1.4 ธนาคารพาณิชย์จะมีการดำเนินการจัดหางบประมาณในการต่ออายุการใช้งานซอฟต์แวร์ลิขสิทธิ์ของอุปกรณ์ในการควบความปลอดภัยระบบเครือข่าย ประกอบด้วยไฟล์วอลล์ ระบบตรวจจับการบุกรุก (Intrusion

Detection System) อย่างต่อเนื่อง เพราะอุปกรณ์ดังกล่าวจำเป็นจะต้องมีการปรับฐานข้อมูลให้ทันสมัย ในการตรวจจับการบุกรุก และการป้องการบุกรุก

5.1.5 ธนาคารพาณิชย์จะมีการเพิ่มอุปกรณ์ในการบริหารจัดการระบบเครือข่ายไร้สายจากศูนย์กลาง (Wireless LAN Centralize Management) และจะมีการดำเนินการทำระบบการยืนยันตัวบุคคลอย่างบูรณาการโดยการใช้แอคทีฟไดเรคทอรี่เป็นเครื่องมือช่วยในการควบคุมผู้เข้าใช้งานผ่านระบบเครือข่ายไร้สายจากส่วนกลาง (Windows Server 2019 Services and Counters, 2019) แต่อย่างไรก็ตามอุปกรณ์ส่งสัญญาณเครือข่ายไร้สายที่มีอยู่เดิมอาจไม่รองรับการทำงานร่วมกับแอคทีฟไดเรคทอรี่ ดังนั้นจึงต้องการจัดหางบประมาณในส่วนดังกล่าวเพิ่มเติม

5.1.6 ธนาคารพาณิชย์จะมีการดำเนินการปรับปรุงให้อุปกรณ์ระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายมีการทำงานแบบไฮเปอร์คอนเวอจ์อินฟราสตรัคเจอร์ คือการใช้ซอฟต์แวร์มาช่วยในการจัดการกับเครื่องคอมพิวเตอร์แม่ข่ายหลาย ๆ ตัวโดยเครื่องคอมพิวเตอร์แม่ข่ายมาทำงานร่วมกันแล้วบริหารทั้งระบบเสมือนเป็นเพียงเครื่องคอมพิวเตอร์แม่ข่ายใหญ่ ๆ เพียงเครื่องเดียว โดยเมื่อระบบทำงานได้ไม่สมบูรณ์หรือระบบล่มบ่อย ๆ ก็สามารถแก้ไขได้โดยการเพิ่มเครื่องคอมพิวเตอร์แม่ข่ายเพิ่มเข้าไปในระบบ และเมื่อมีเครื่องคอมพิวเตอร์แม่ข่ายมีปัญหาหรือเสียก็จะมีเครื่องมาทำงานแทนโดยอัตโนมัติ ทั้งหมดนี้ผ่านการบริหารจัดการผ่านบัญชีผู้ใช้เดียวกันไม่ต้องมีชื่อบัญชีผู้ใช้งานและรหัสผ่านจำนวนมากแยกตามอุปกรณ์หรือระบบ

5.2 ด้านผู้ปฏิบัติงาน

5.2.1 ธนาคารพาณิชย์จะมีการดำเนินการเร่งจัดทำแบบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงทางไซเบอร์ของธนาคารพาณิชย์โดยการกำหนดเป็นแนวนโยบายและปฏิบัติที่เป็นลายลักษณ์อักษรในการมอบอำนาจหน้าที่ในการปฏิบัติตามลำดับชั้น

5.2.2 ธนาคารพาณิชย์จะมีการดำเนินการให้ความสำคัญกับเข้าถึงระบบสารสนเทศผ่านเครือข่ายไร้สายทั้งรูปแบบการให้บริการแก่บุคคลภายนอก และภายในโดยมีการเก็บข้อมูลการเข้าใช้ และข้อมูลผู้ใช้อย่างเป็นระบบผ่านอุปกรณ์จัดเก็บข้อมูลบันทึกเหตุการณ์ใช้งาน (Log File) อีกทั้งในกรณีที่มีกำหนดรหัสเข้าใช้งานแบบไม่อัตโนมัติ และมีการเปลี่ยนรหัส หรือปรับเปลี่ยนวิธีการเข้ารหัสข้อมูลอย่างน้อยเดือนละหนึ่งครั้ง

5.3 ด้านภัยหรือสถานการณ์ฉุกเฉิน

5.3.1 ธนาคารพาณิชย์จะมีการดำเนินการเร่งจัดทำแบบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงทางไซเบอร์ของธนาคารพาณิชย์เพื่อเป็นกรอบแนวทางในการการรักษาความมั่นคงทางไซเบอร์เป็นลายลักษณ์อักษรเพื่อให้เป็นแนวปฏิบัติในการดำเนินการด้านการสำรองระบบฐานข้อมูลตามรอบการทำงานปกติ เช่น การสำรองฐานข้อมูลอาทิตย์ละ 1 ครั้ง และการสร้างศูนย์ข้อมูลสำรอง (Disaster Recovery Site) (สุพิชญา อาชวิรดา, 2559) ที่สามารถแก้ไขปัญหาระบบสารสนเทศที่เกิดขึ้นจากภัยพิบัติต่าง ๆ ให้สามารถทำงานได้อย่างทันท่วงที

5.4 ด้านการบริหารจัดการ

5.4.1 ผู้บริหารธนาคารพาณิชย์จะมีการดำเนินการเร่งจัดทำแบบนโยบายและแนวปฏิบัติในการรักษาความมั่นคงทางไซเบอร์ของธนาคารพาณิชย์เพื่อเป็นกรอบแนวทางในการการรักษาความมั่นคงทางไซเบอร์เป็นลายลักษณ์อักษรเพื่อการสร้างความรับรู้และตระหนักแก่ผู้บริหารระดับสูงสุดของหน่วยงาน เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

5.4.2 ธนาคารพาณิชย์จะมีการดำเนินการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง และในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วยงาน หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอกเพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงทางไซเบอร์ของธนาคาร นอกเหนือจากการตรวจสอบและประเมินความเสี่ยงที่เป็นกรอบการบริหารจัดการองค์กรที่มีอยู่แล้ว

5.5 การประเมินค่าความเสี่ยง

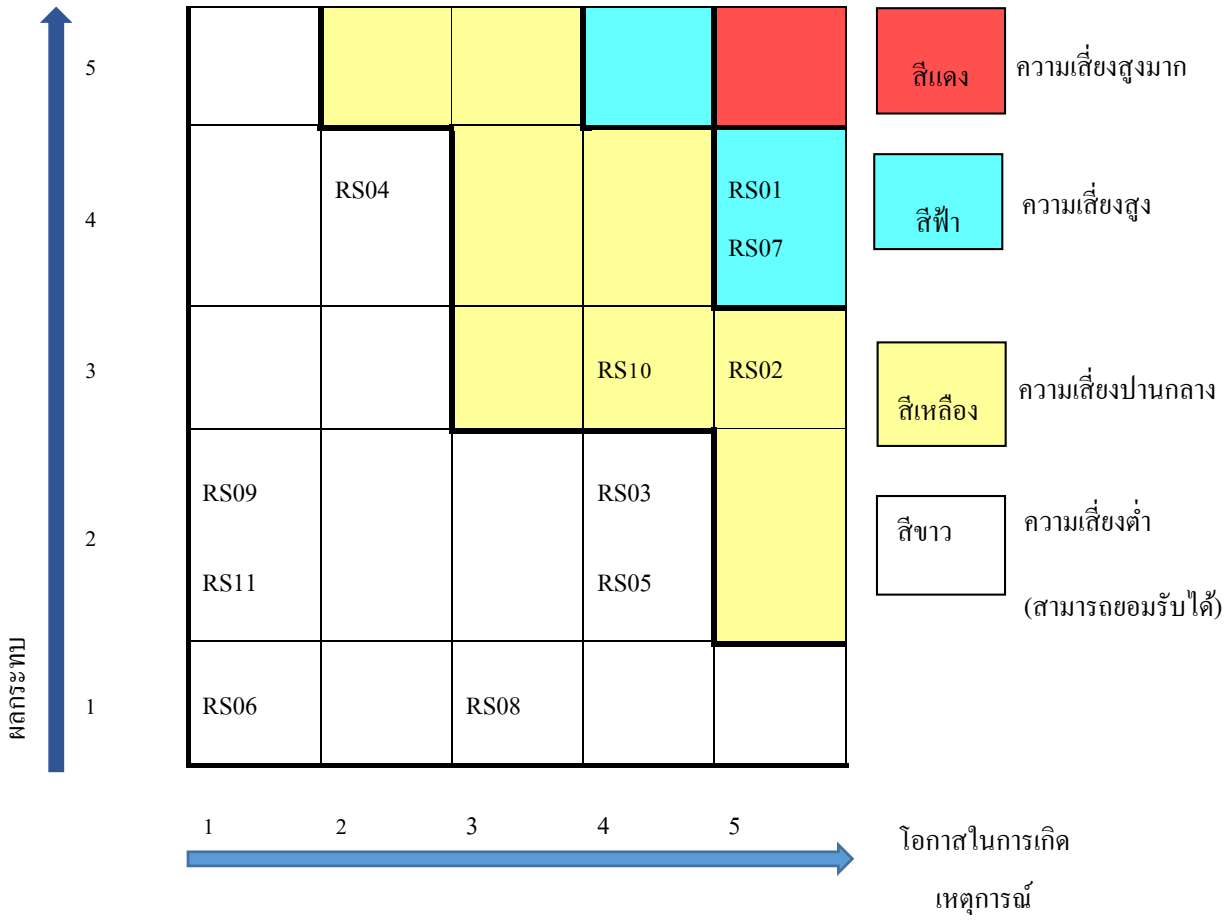
การประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสามารถสรุปเป็นแผนภูมิความเสี่ยงแสดงดังรูปที่ 1 และสรุปรายละเอียดการประเมินค่าความเสี่ยงแยกประเภทความเสี่ยงดังตารางที่ 2 โดยมีการแบ่งประเภทความเสี่ยง ดังนี้

5.5.1 ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย เครื่องมือ และอุปกรณ์ อาจเกิดถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี หรือถูกก่อกวนจากผู้ประสงค์ร้าย ถูกเจาะทำลายระบบ เป็นต้น

5.5.2 ความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่าง ๆ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้ (เอกฉัตร บ่ายคล้อย และประสงค์ ประณีตพลกรัง, 2560)

5.5.3 ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

5.5.4 ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการวางแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ



รูปที่ 1 แผนภูมิความเสี่ยง

ตารางที่ 2 สรุปการประเมินค่าความเสี่ยง

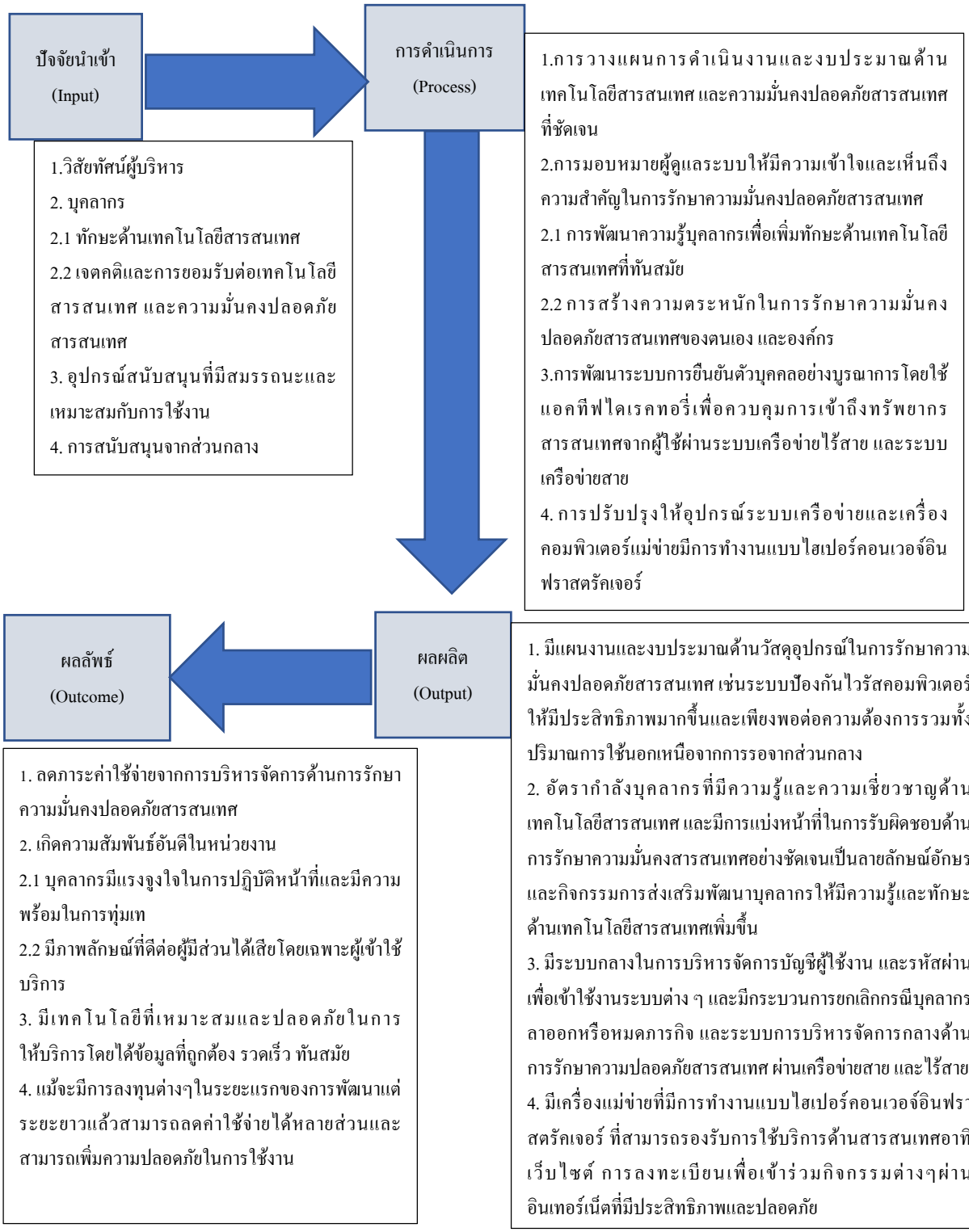
ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	โอกาสในการเกิดเหตุการณ์ x ผลกระทบ	ระดับความเสี่ยง
1. ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	RS01	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	5x4	20

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	โอกาสในการเกิดเหตุการณ์ x ผลกระทบ	ระดับความเสี่ยง
2. ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	RS02	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการใช้ระบบเครือข่าย เช่น การนำอุปกรณ์เชื่อมต่อสัญญาณแบบไร้สาย (wireless router) หรือสวิตช์ (switch/hub) มาเชื่อมต่อกับระบบเครือข่ายส่วนกลาง โดยไม่ได้รับอนุญาต และไม่ได้มีการตั้งค่าเครื่องที่ถูกต้อง ทำให้เครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายไม่สามารถใช้งานได้ง่าย	5x3	15
3. ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	RS03	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	ธนาคารมีระบบสำรองไฟของระบบเครือข่ายและเครื่องแม่ข่าย แต่ไม่ระบบสำรองไฟให้แก่ผู้ใช้งานรายบุคคลทำให้เมื่อเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่	4x2	8
4. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี	RS04	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	2x4	8
5. ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	RS05	ความเสี่ยงด้านการบริหารจัดการ	จำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	4x2	8

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง		ระดับคะแนน
6. ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	RS06	ความเสี่ยงด้านการบริหารจัดการ	การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ	1x1	1
7. ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	RS07	ความเสี่ยงด้านการบริหารจัดการ	การขาดแคลนงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	5x4	20
8. ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	RS08	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	3x1	3
9. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	RS09	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	1x2	2
10. ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	RS10	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดหรือขัดข้องด้วยสาเหตุทางเทคนิค หรือจากสัตว์กัดแทะเช่น หนูหรือแมลง เป็นต้น	4x3	12
11. ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	RS11	ความเสี่ยงด้านการบริหารจัดการ/ความเสี่ยงจากผู้ปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	1x2	2

6. บทสรุป

จากการวิเคราะห์การรักษาความมั่นคงทางไซเบอร์ของธนาคารพาณิชย์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 จะพบว่าธนาคารพาณิชย์นี้จะต้องมีการปรับปรุงพัฒนาเพื่อสร้างเข้มแข็งในด้านเทคโนโลยีสารสนเทศกันครบทั้ง 3 ด้านคือ 1) การใช้เทคโนโลยีที่เหมาะสมสำหรับการบูรณาการในด้านเทคนิค เช่น การยืนยันตัวบุคคลอย่างบูรณาการ ไฮเปอร์คอนเวอจ์อินฟราสตรัคเจอร์ หรือการพัฒนาคลังข้อมูลกลาง 2) มีการสร้างแบบนโยบายหรือแนวทางปฏิบัติสำหรับกำกับผู้ปฏิบัติงานเพื่อลดความเสี่ยงหรือภัยคุกคามที่มาจากความผิดพลาดของมนุษย์ และ3) มีการเตรียมความพร้อมหรือมีมาตราการรองรับสำหรับด้านภัยหรือสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้น ทั้งนี้สามารถสรุปแนะแนวทางการป้องกันภัยคุกคามให้สอดคล้องกับตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้ดังรูปที่ 2



รูปที่ 2 สรุปแนวทางการป้องกันภัยคุกคามของธนาคารพาณิชย์

7. กิตติกรรมประกาศ

ผู้วิจัยขอขอบพระคุณ ผศ.ดร.เชฏฐเนติ ศรีสอ้าน คณบดี วิทยาลัยนวัตกรรมดิจิทัลและเทคโนโลยีสารสนเทศ มหาวิทยาลัยรังสิต ที่ให้การสนับสนุน และอำนวยความสะดวกในการจัดทำการวิจัย และธนาคารกรุงศรีอยุธยาจำกัด (มหาชน) ที่ให้ข้อมูลพื้นฐานด้านระบบสารเทศของธนาคารพาณิชย์

8. เอกสารอ้างอิง

พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562. (2562, 22 พฤษภาคม). ราชกิจจานุเบกษา. เล่มที่ 136 ตอนที่ 67 ก.

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (2562, 27 พฤษภาคม). ราชกิจจานุเบกษา. เล่มที่ 136 ตอนที่ 69 ก.

สุพิชญา อาชวิรดา. (2559). ปัจจัยที่ส่งผลต่อระดับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร. *วารสารระบบสารสนเทศด้านธุรกิจ. 2*(2), เมษายน – มิถุนายน, 66-79.

อรรถพล ป้อมสถิตย์. (2561). Computer and Information Security Theory. (พิมพ์ครั้งที่ 1). กรุงเทพมหานคร: สำนักพิมพ์มหาวิทยาลัยราชภัฏสวนสุนันทา.

อินทัช โฮลดิ้งส์ จำกัด (มหาชน). (2560). นโยบายการรักษาความมั่นคงทางไซเบอร์. สืบค้นจาก https://www.intouchcompany.com/privacy_th.asp.

เอกฉัตร บ่ายคล้อย และประสงค์ ประณีตพลกรัง. (2560). ความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศ ในระบบประมวลผลแบบคลาวด์. *วารสารสหศาสตร์ศรีปทุม ชลบุรี. 3*(2). 22-29.

National Institute of Standards and Technology (NIST). (2018). Cybersecurity Framework Version 1.1. Retrieved from https://www.nist.gov/cyberframework.

Sverdlik, Y. (2015). Why Hyperconverged Infrastructure is so Hot. Retrieved from https://www.datacenterknowledge.com/archives/2015/12/10/why-hyperconverged-infrastructure-is-so-hot.

Windows Server 2019 Services and Counters. (online). Retrieved from https://documentation.solarwinds.com/en/Success_Center/SAM/Content/SAM-Windows-Server-2019-Services-and-Counters.htm.