การพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง

THE DEVELOPMENT OF CYBERSECURITY FRAMEWORK FOR INTERNET OF THINGS

วิลาส วิถีไพร

WILAS WITHEEPRAI

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยศรีปทุม
พ.ศ. 2561

การพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง

วิลาส วิถีไพร

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยศรีปทุม
พ.ศ. 2561

THE DEVELOPMENT OF CYBERSECURITY FRAMEWORK FOR INTERNET OF THINGS

WILAS WITHEEPRAI

A THEMATIC SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

SCHOOL OF INFORMATION TECHNOLOGY

SRIPATUM UNIVERSITY

2018

หัวข้อสารนิพนธ์	การพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง THE DEVELOPMENT OF CYBERSECURITY FRAMEWORK FOR INTERNET OF THINGS
นักศึกษา	วิลาส วิถีไพร รหัสประจำตัว 60501164
หลักสูตร	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะ	เทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
อาจารย์ที่ปรึกษาสารนิพนธ์	ผู้ช่วยศาสตราจารย์ ดร.นิเวศ จิระวิชิตชัย
อาจารย์ที่ปรึกษาสารนิพนธ์ร่วม	ศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง

คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม อนุมัติให้นับสารนิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะเทคโนโลยีสารสนเทศ
(ผู้ช่วยศาสตราจารย์ ดร.ธนา สุขวารี)

วันที่.....เดือน.....พ.ศ. .....

คณะกรรมการการสอบสารนิพนธ์

..... ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ประณต บุญไชยอภิสิทธิ์)

..... กรรมการ
(ศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.นิเวศ จิระวิชิตชัย)

สารนิพนธ์เรื่อง การพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง
คำสำคัญ อินเทอร์เน็ตประสานสรรพสิ่ง ความมั่นคงปลอดภัยไซเบอร์ ภัยคุกคามทางไซเบอร์
นักศึกษา นายวิลาส วิถีไพร
อาจารย์ที่ปรึกษา ผู้ช่วยศาสตราจารย์ ดร.นิเวศ จิระวิชิตชัย
อาจารย์ที่ปรึกษาร่วม ศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง
หลักสูตร วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะวิชา บัณฑิตวิทยาลัย มหาวิทยาลัยศรีปทุม
พ.ศ. 2561

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์ 1) เพื่อศึกษาและวิเคราะห์ภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง 2) เพื่อพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง และ 3) เพื่อพัฒนาแอปพลิเคชันระบบประเมินความเสี่ยงด้านภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง ผู้วิจัยได้ใช้แบบสอบถามสำหรับสัมภาษณ์เชิงลึกผู้เชี่ยวชาญ จำนวน 7 คน ผลการวิจัยพบว่า อินเทอร์เน็ตประสานสรรพสิ่งมีความเสี่ยงมาก เนื่องจากยังไม่มีมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ดี และแบบสอบถามปลายปิดสำหรับบุคลากรของกองวิศวกรรมและแผนงาน การไฟฟ้าส่วนภูมิภาค เขต 1 (ภาคใต้) จังหวัดเพชรบุรี จำนวน 40 คน ผลการวิจัยพบว่า ความคิดเห็นเกี่ยวกับความเสี่ยงของภัยคุกคามทางไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่งอยู่ในระดับปานกลาง

จากการวิเคราะห์ข้อมูลที่ได้ ประกอบกับการอ้างอิงกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ สหรัฐอเมริกา ผู้วิจัยจึงทำการพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง พร้อมทั้งพัฒนาแอปพลิเคชันสำหรับประเมินองค์กรถึงความเสี่ยงด้านภัยคุกคามทางไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง ซึ่งจะทำให้องค์กรสามารถเตรียมความพร้อมและปรับปรุงนโยบายด้านความมั่นคงปลอดภัยไซเบอร์สำหรับการใช้อินเทอร์เน็ตประสานสรรพสิ่งในองค์กรได้

THEMATIC TITLE	THE DEVELOPMENT OF CYBERSECURITY FRAMEWORK FOR INTERNET OF THINGS
KEYWORDS	INTERNET OF THINGS, CYBERSECURITY, CYBER THREATS
STUDENT	MR.WILAS WITHEEPRAI
ADVISOR	ASSIST. PROF. DR.NIVET CHIRAWIVHITCHAI
CO-ADVISOR	PROF. DR.PRASONG PRANEETPOLGRANG
LEVEL OF STUDY	MASTER OF SCIENCE IN INFORMATION TECHNOLOGY
FACULTY	SCHOOL OF INFORMATION TECHNOLOGY SRIPATUM UNIVERSITY
YEAR	2018

ABSTRACT

This research is aimed to 1) study and analyze the cyber threats and risks that affect Internet of Things, 2) to develop the cybersecurity framework for Internet of Things, 3) to develop the application in threats and cyber threats of the risk assessment application which affects Internet of Things. The researchers used a questionnaire for comprehensive interviews with 7 experts. The research found that the Internet of Things was highly risk because there was the best reasonably non-standard for cyber security, including the closed questionnaires for 40 personnel of engineering and planning departments, Provincial Electricity Authority, Area 1 (South), Phetchaburi. The results of the research were comments on the risk of cyber threats for Internet of Things in moderate level.

Based on data analysis and some references to the cybersecurity framework of the National Institute of Standards and Technology, USA, the researchers have developed a cybersecurity framework for Internet of things. It also develops applications for assessing the organization's potential cyber threats which affect Internet of Things. This will enable organizations to prepare and improve their cybersecurity policies for Internet of Things use, increasingly.

กิตติกรรมประกาศ

ผู้วิจัยขอขอบพระคุณผู้มีพระคุณทุกท่านที่มีส่วนช่วยให้สารนิพนธ์ฉบับนี้สำเร็จลุล่วงดังความประสงค์ที่ได้ตั้งใจไว้ ผู้วิจัยขอขอบพระคุณ พ่อแม่ ญาติ พี่น้อง ที่ได้ให้การสนับสนุน ขอขอบพระคุณท่านอาจารย์ที่ปรึกษา ศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง และผู้ช่วยศาสตราจารย์ ดร.นิเวศ จิระวิชิตชัย ที่ได้ให้คำชี้แนะและเสริมสร้างความมุ่งมั่นด้านวิชาการ ขอขอบพระคุณคณาจารย์ทุกท่านที่ได้ให้ความรู้ ขอขอบพระคุณผู้เชี่ยวชาญ และบุคลากรของกองวิศวกรรมและแผนงาน การไฟฟ้าส่วนภูมิภาค เขต 1 (ภาคใต้) จังหวัดเพชรบุรี ที่ได้กรุณาให้สัมภาษณ์และตอบแบบสอบถาม ขอขอบพระคุณมหาวิทยาลัยศรีปทุมที่ช่วยส่งเสริมทรัพยากรสำหรับการเรียนรู้ตลอดชีวิต ขอขอบพระคุณเจ้าหน้าที่ทุกท่านที่ช่วยอำนวยความสะดวกระหว่างการศึกษา ขอขอบพระคุณเพื่อนร่วมรุ่น รุ่นพี่ รุ่นน้อง ทุกท่าน ที่ช่วยเป็นกำลังใจและให้คำปรึกษา เป็นอย่างดี ตั้งแต่เริ่มต้น จนกระทั่งสารนิพนธ์ฉบับนี้สำเร็จ

ผู้วิจัยหวังเป็นอย่างยิ่งว่าจะนำความรู้ที่ได้รับจากการศึกษาไปสร้างคุณประโยชน์แก่สังคม ประเทศชาติ จึงขอขอบพระคุณผู้มีพระคุณทุกท่านมา ณ โอกาสนี้

วิลาส วิถีไพร

สารบัญ

บทที่ หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญภาพ

ภาพประกอบที่ หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

อินเทอร์เน็ตประสานสรรพสิ่ง (Internet of things: IoT) ได้รับการยอมรับอย่างรวดเร็วว่ามีบท บาทสำคัญที่ช่วยปรับปรุงการดำเนินชีวิตประจำวันให้มีความหลากหลายอย่างมีประสิทธิภาพมากขึ้น (ACM, 2017) ในช่วงไม่กี่ปีที่ผ่านมา อินเทอร์เน็ตประสานสรรพสิ่ง มีเสน่ห์ดึงดูดใจของผู้คน เนื่องจากมีศักยภาพในการเปลี่ยนแปลงวิถีชีวิตและการดำเนินธุรกิจได้อย่างรวดเร็ว อินเทอร์เน็ตประสานสรรพสิ่งประกอบด้วยอุปกรณ์ (รวมทั้งเซนเซอร์) ที่โต้ตอบสื่อสารกับเครื่องจักร วัตถุ และสภาพแวดล้อมอื่น ๆ และสร้างเป็นระบบนิเวศอัจฉริยะ (Pathak, 2017) คำว่า “อินเทอร์เน็ตประสานสรรพสิ่ง หรือ Internet of Things” เป็นคำที่ใช้ในปัจจุบันเพื่ออธิบายถึงการผสมผสานกัน ระหว่างเครื่องจักรและเทคโนโลยีการดำเนินงาน (Operation Technology) เทคโนโลยีสารสนเทศ (Information Technology) สภาพแวดล้อมทางกายภาพ และผู้ใช้งาน ซึ่ง ISO/IEC ได้ให้คำจำกัดความไว้ว่า “IoT คือ โครงสร้างพื้นฐานของวัตถุที่เชื่อมต่อกับผู้คน ระบบและแหล่งข้อมูล พร้อมด้วยการบริการอัจฉริยะเพื่อให้สามารถประมวลผลข้อมูลของโลกทางกายภาพและโลกเสมือนจริง และนำมาปรับใช้” (Damiani et al, 2018) ภายในปี 2020 จะมีอุปกรณ์ IoT จำนวน 24 พันล้านเครื่อง ติดตั้งอยู่ทั่วโลก คาดว่าแต่ละวันในปีนี้จะมีการเชื่อมต่ออุปกรณ์ IoT ชนิดใหม่ๆ จำนวนถึง 5.5 ล้านชนิด IoT จะห้อมล้อมอยู่ในชีวิตประจำวันของผู้คน ในด้านการดำเนินชีวิตและการสื่อสาร (Mehta, 2017) จะมีข้อมูลจำนวนมาก รับ-ส่ง ประมวลผล จัดเก็บ เพื่อนำไปใช้งานอย่างมีประสิทธิภาพ (Alsaadi and Tubaishat, 2015) เป็นการแลกเปลี่ยนข้อมูลกันระหว่างผู้ใช้ที่เป็นมนุษย์ กับคอมพิวเตอร์แต่ละเครื่อง ภายใต้โครงสร้างพื้นฐานทางกายภาพและอินเทอร์เน็ตที่เชื่อมต่อกัน (Ochoa et al., 2017) ซึ่งในแต่ละอุปกรณ์จะมี Ip Address ประจำเครื่อง ทำให้เกิดความเสี่ยงที่ผู้ประสงค์ร้ายจะทำการแฮ็กอุปกรณ์ได้ (TRIPWIRE GUEST AUTHORS, 2016) จึงเป็นเรื่องสำคัญที่ควรปกป้องการเข้าถึงอุปกรณ์อินเทอร์เน็ตประสานสรรพสิ่งอย่างเร่งด่วน (Liang et al., 2018)

อินเทอร์เน็ตประสานสรรพสิ่งสามารถเชื่อมต่ออุปกรณ์ต่าง ๆ ได้หลากหลายอุปกรณ์ เช่น คอมพิวเตอร์ส่วนบุคคล โทรศัพท์มือถือ และเครื่องพิมพ์ ถือว่าเป็นอุปกรณ์อินเทอร์เน็ตประสานสรรพสิ่งแบบดั่งเดิมเนื่องจากมีการใช้งานในระบบเครือข่ายในอดีต (Mavropoulos et al., 2017) เป็นที่คาดหวังว่าเทคโนโลยีอินเทอร์เน็ตประสานสรรพสิ่งจะเปิดโอกาสในการสร้างแอปพลิเคชันรูปแบบใหม่ ๆ ในหลากหลายศาสตร์ เช่น ด้านการดูแลสุขภาพ ด้านการรักษาความมั่นคงปลอดภัยและการตรวจตรา ด้านการขนส่ง ด้านอุตสาหกรรม และบูรณาการเทคโนโลยี ในด้านการสื่อสารแบบ Machine-to-Machine ขั้นสูง เครือข่ายอัตโนมัติ การช่วยในการตัดสินใจ ความมั่นคงปลอดภัยและการปกป้องความเป็นส่วนตัว และด้านคลาวน์คอมพิวติ้ง ร่วมด้วยเทคโนโลยีการตรวจจับและตัวกระตุ้นขั้นสูง (Oracevic et al., 2017) หัวข้อที่ท้าทายที่สุดในระบบการเชื่อมต่อของวัตถุก็คือด้านความมั่นคงปลอดภัยและความเป็นส่วนตัว (Liu et al., 2012) โดยเฉพาะการที่อุปกรณ์อินเทอร์เน็ตประสานสรรพสิ่งมีคุณสมบัติที่เป็นจุดเด่นคือมีความคล่องตัว นำไปใช้งานได้กับสภาพแวดล้อมที่หลากหลาย สามารถเชื่อมต่อกับอุปกรณ์อื่น และมีแพลตฟอร์มที่แตกต่างกัน ทำให้การติดตั้งทรัพยากรจำนวนมากไม่เหมาะสมกับบริบทการใช้งาน หรือไม่สามารถติดตั้งทรัพยากรด้านความมั่นคงปลอดภัยที่เพียงพอเข้าไปในอุปกรณ์อินเทอร์เน็ตประสานสรรสิ่งได้ (Krishna and Gnanasekaran, 2017)

อินเทอร์เน็ตประสานสรรพสิ่งเป็นเทคโนโลยีที่มีความสำคัญและได้รับความนิยมมากขึ้นเรื่อย ๆ เนื่องจากอำนวยความสะดวกและนำไปใช้ประโยชน์ได้อย่างกว้างขวาง (สรวิศ, 2018) การรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอุปกรณ์อินเทอร์เน็ตประสานสรรพสิ่งควรทำให้ครอบคลุมในทุก ๆ ด้าน ทั้งในด้านอุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์ การเชื่อมต่อ เริ่มตั้งแต่กระบวนการผลิตไปจนถึงการสร้างความตระหนักให้แก่ผู้ใช้งาน ผู้ผลิตจะต้องมีจะต้องมีบริการหลังการขายในเรื่องการติดตั้ง patch ที่ได้รับการรับรองและทันต่อเหตุการณ์ภัยคุกคาม ทุกอุปกรณ์ต้องใช้รหัสผ่านที่สามารถเปลี่ยนแปลงได้ (Schneier, 2017) ซึ่งในปัจจุบันยังไม่มีมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่งที่ชัดเจน ผู้ใช้งานส่วนมากยังคงไม่ตระหนักถึงภัยคุกคามจากการใช้งาน ดังนั้นผู้วิจัยจึงมีความสนใจพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง เพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย

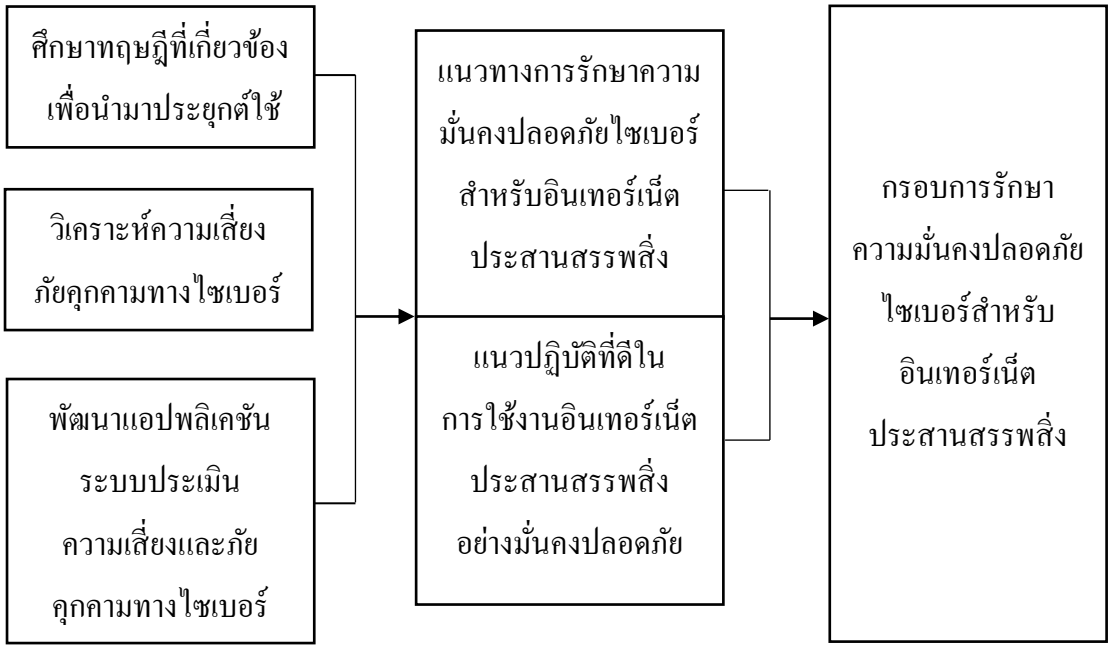
1.2 วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาและวิเคราะห์ภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง

2. เพื่อพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง

3. เพื่อพัฒนาแอพพลิเคชันระบบประเมินความเสี่ยงด้านภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง

1.3 กรอบแนวคิดการวิจัย



ภาพประกอบที่ 1.1 กรอบแนวคิดการวิจัย

1.4 คำถามการวิจัย

ทำอย่างไรจึงจะสามารถลดความเสี่ยงและภัยคุกคามทางไซเบอร์ได้ เพื่อให้ใช้งานอินเทอร์เน็ตประสานสรรพสิ่งได้อย่างมั่นคงปลอดภัย

1.5 สมมุติฐานการวิจัย

การพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง สามารถลดความเสี่ยงและภัยคุกคามทางไซเบอร์จากการใช้งานอินเทอร์เน็ตประสานสรรพสิ่งได้

1.6 ขอบเขตการวิจัย

การวิจัยในครั้งนี้เป็นการพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยการวิเคราะห์ภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง เพื่อนำข้อมูลที่ได้มาจัดทำแนวปฏิบัติที่ดีในการใช้งาน และพัฒนาแอปพลิเคชันสำหรับประเมินความเสี่ยงด้านภัยคุกคามทางไซเบอร์ สำหรับองค์กรที่ใช้งานอินเทอร์เน็ตประสานสรรพสิ่ง

1.7 ประโยชน์ที่ได้รับจากการวิจัย

1. ทำให้ได้ทราบถึงภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง

2. ทำให้ทราบถึงกรอบวิธีปฏิบัติและแนวทางในการใช้งานอินเทอร์เน็ตประสานสรรพสิ่งอย่างมั่นคงปลอดภัย

3. ทำให้องค์กรได้แนวทางและเตรียมการป้องกันความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง

1.8 นิยามศัพท์

อินเทอร์เน็ตประสานสรรพสิ่ง (Internet of things: IoT) คือ การที่สิ่งต่าง ๆ ถูกเชื่อมโยงทุกสิ่งทุกอย่างเข้าสู่โลกอินเทอร์เน็ต ทำให้มนุษย์สามารถสั่งการ ควบคุมใช้งานอุปกรณ์ต่าง ๆ ผ่านทางเครือข่ายอินเตอร์เน็ต เช่น การสั่งเปิด-ปิด อุปกรณ์เครื่องใช้ไฟฟ้า รถยนต์ โทรศัพท์มือถือ เครื่องมือสื่อสาร เครื่องใช้สำนักงาน เครื่องมือทางการเกษตร เครื่องจักรในโรงงานอุตสาหกรรม อาคาร บ้านเรือน เครื่องใช้ในชีวิตประจำวันต่าง ๆ ผ่านเครือข่ายอินเทอร์เน็ต เป็นต้น

ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) หมายความว่า มาตรการและการดำเนินการที่กำหนดขึ้นเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศให้สามารถปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการ

ให้บริการโดยปกติของดาวเทียม อันกระทบต่อความมั่นคงของชาติรวมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ

ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า ภัยคุกคามใหญ่หลวงต่อผลประโยชน์ทางเศรษฐกิจ ตลอดจนความมั่นคงของประเทศ การโจมตีทางไซเบอร์มีหลายรูปแบบ เช่น การเจาะระบบคอมพิวเตอร์ (Hacking) การสอดแนมข้อมูลคอมพิวเตอร์โดยสปายแวร์ การดักรับข้อมูลคอมพิวเตอร์ (Sniffing) การโจมตีโดยชุดคำสั่งไม่พึงประสงค์ (Malicious Software: Malware) หรือการรุมสอบถามข้อมูลจนระบบล่ม (Denial of Service Attack: DOS) เป็นต้น

กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ สหรัฐอเมริกา (National Institute of Standards and Technology: NIST) คือ กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วยมาตรฐาน แนวทาง วิธีปฏิบัติที่ดี เพื่อจัดการด้านความมั่นคงปลอดภัยไซเบอร์และความเสี่ยงที่เกี่ยวข้อง ช่วยจัดลำดับความสำคัญ ยืดหยุ่น และลดค่าใช้จ่ายในการป้องกันและฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์สำหรับโครงสร้างพื้นฐานและส่วนอื่น ๆ ที่สำคัญ ของความมั่นคงปลอดภัยทางเศรษฐกิจและประเทศ

บทที่ 2
แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

การศึกษาสารนิพนธ์ เรื่อง การพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง ผู้ศึกษาวิจัยได้ทำการรวบรวมข้อมูลแนวคิดทฤษฎีที่เกี่ยวข้องและศึกษาเอกสารงานวิจัย ดังนี้

2.1 อินเทอร์เน็ตประสานสรรพสิ่ง (Internet of Things: IoT)

2.2 มาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Systems: ISO 27001:2013)

2.3 การประเมินการปฏิบัติการเกี่ยวกับช่องโหว่และสินทรัพย์ ภัยคุกคามที่สำคัญยิ่งยวด (Operationally Critical Threat, Asset and Vulnerability Evaluation: OCTAVE)

2.4 กรอบการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานที่สำคัญยิ่งยวด (Framework for Improving Critical Infrastructure Cybersecurity)

2.5 งานวิจัยที่เกี่ยวข้อง

2.1 อินเทอร์เน็ตประสานสรรพสิ่ง (Internet of Things: IoT)

Internet of Things (IoT) หมายถึง การที่สิ่งต่าง ๆ ถูกเชื่อมโยงทุกสิ่งทุกอย่างเข้าสู่โลกอินเทอร์เน็ต ทำให้มนุษย์สามารถสั่งการ ควบคุมใช้งานอุปกรณ์ต่าง ๆ ผ่านทางเครือข่ายอินเทอร์เน็ต เช่น กำรสั่งเปิด-ปิด อุปกรณ์เครื่องใช้ไฟฟ้า รถยนต์ โทรศัพท์มือถือ เครื่องมือสื่อสาร เครื่องใช้สำนักงาน เครื่องมือทางการเกษตร เครื่องจักรในโรงงานอุตสาหกรรม อาคาร บ้านเรือน เครื่องใช้ในชีวิตประจำวันต่าง ๆ ผ่านเครือข่ายอินเทอร์เน็ต

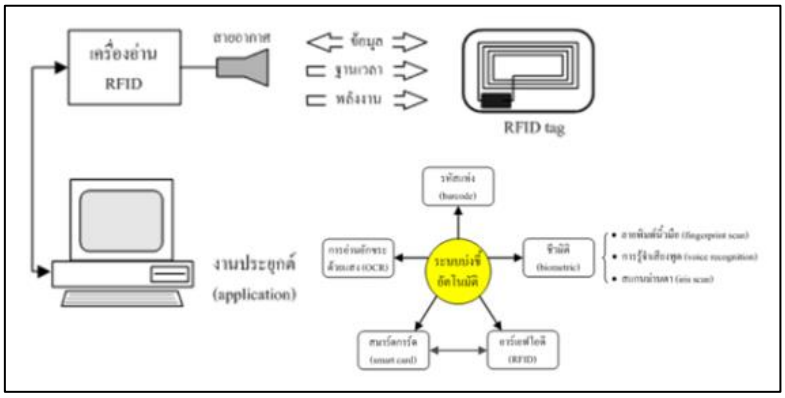
หรือบางแห่งเรียก M2M ย่อมาจาก Machine to Machine คือ เทคโนโลยีอินเทอร์เน็ตที่เชื่อมอุปกรณ์ กับเครื่องมือต่าง ๆ เช่น โทรศัพท์มือถือ รถยนต์ ตู้เย็น โทรทัศน์ และอื่น ๆ เข้าไว้ด้วยกัน โดยการเชื่อมโยงช่วยให้สื่อสารกันได้ผ่านระบบอินเทอร์เน็ต เป็นต้น

ในยุค ค.ศ. 1980 - 1990 ที่เหล่านักวิศวกร รวมถึงนักวิทยาศาสตร์ได้คิดค้น พัฒนาเครื่องมือต่าง ๆ ขึ้นมาให้เชื่อมโยงกับอีกสิ่งหนึ่ง เพื่ออำนวยความสะดวกในการติดต่อสื่อสาร และการใช้ชีวิตประจำวัน ด้วยเทคโนโลยีในขณะนั้น ผนวกกับต้นทุนที่สูงจนเกินไป ทำให้แนวคิดดังกล่าวไม่เป็นที่นิยมเท่าไรนัก เมื่อวันเวลาเปลี่ยนไปก็เข้าสู่ยุคที่เทคโนโลยีมีความเจริญก้าวหน้า การติดต่อสื่อสารของเครื่องไม้เครื่องมือระหว่างกันก็เริ่มประจักษ์ให้เห็นมากขึ้น จากการใช้ "คลื่น RFID" หรือที่รู้จักกันว่าคลื่นวิทยุนั่นเอง

สำหรับ RFID ก็มีจุดเริ่มต้นมาอย่างยาวนานเช่นกัน โดยต้องย้อนกลับไปในสมัยสงครามโลกครั้งที่ 2 มีนักฟิสิกส์ชาวสกอตแลนด์นามว่า Sir Robert Alexander Watson-Watt ได้คิดค้นเทคโนโลยีดังกล่าวขึ้นมา เพื่อตรวจจับเครื่องบิน และเตือนเมื่อมีเครื่องบินเข้ามา จากนั้นก็พัฒนาเรื่อยมาให้มีระยะไกลขึ้น รวมถึงมีความเที่ยงตรง ถูกต้องแม่นยำ ปลอดภัย ทนต่อสภาวะแวดล้อม และสุดท้ายก็ถูกนำไปใช้ในอุตสาหกรรม หรือธุรกิจต่าง ๆ อย่างแพร่หลายในระยะเวลาอันรวดเร็ว จนกระทั่งได้รับความนิยมไปทั่วโลก

ในขณะนั้นหนึ่งในเทคโนโลยีใหม่ที่น่าจับตามอง และจะปฏิวัติการติดต่อสื่อสารก็คืออินเทอร์เน็ต "Internet" ก้าวเข้ามาเป็นส่วนสำคัญ รวมถึงเริ่มแพร่หลายในชีวิตประจำวัน และด้านธุรกิจอย่างรวดเร็ว ด้วยประโยชน์ที่มี อาทิ ความรวดเร็วในการติดต่อสื่อสาร, ต้นทุนต่ำ, แหล่งข้อมูลขนาดใหญ่, เข้าถึงได้ทุกที่ทุกเวลา เป็นต้น ดังนั้นจึงเกิดคำถามว่าทำไมสิ่งของรอบตัวจะสื่อสารกันเองไม่ได้? ผ่านเครือข่ายไร้สาย โดยที่มนุษย์ไม่ต้องเข้าไปเป็นผู้ควบคุมหรือสั่งการทุกกระบวนการหรือที่เรียกกันว่า Internet of things

แนวคิด Internet of Things (ภาพประกอบที่ 2.1) นั้นถูกคิดขึ้นโดย Kevin Ashton ในปี 1999 ซึ่งเขาเริ่มต้นโครงการ Auto-ID Center ที่มหาวิทยาลัย Massachusetts Institute of Technology หรือ MIT จากเทคโนโลยี RFID ที่จะทำให้เป็นมาตรฐานระดับโลกสำหรับ RFID Sensors ต่าง ๆ ที่จะเชื่อมต่อกันได้



ภาพประกอบที่ 2.1 แนวคิด IoT

ต่อมาในยุคหลังปี 2000 โลกมีอุปกรณ์อิเล็กทรอนิกส์ออกมำเป็นจำนวนมากและมีการใช้คำว่า Smart เช่น Smart Device, Smart Grid, Smart Home, Smart Intelligent Transportation

แนวคิดในเรื่องเครือข่ายของ Smart devices ดังกล่าวข้างต้น มีมาตั้งแต่ปี 1982 (2525) โดยมีการสร้างตู้หยอดเหรียญซื้อโค้กที่ Carnegie Mellon University (เดิมชื่อ Carnegie Institute of Technology) ซึ่งประดิษฐกรรมนี้เป็นอุปกรณ์ไฟฟ้าที่เชื่อมต่อกับระบบอินเทอร์เน็ตเครื่องแรกของโลก ตู้นี้สามารถรายงานว่ามีสต็อกเหลืออยู่กี่กระป๋อง กระป๋องที่ใส่เข้าไปเย็นหรือยัง ฯลฯ ในปี 1991 (2534) Mark Weiser เขียนบทความสำคัญชื่อ “The Computer of the 21th Century” และตามมาด้วยงานเขียนของนักวิชาการอีกหลายคนจนเกิดวิสัยทัศน์ในเรื่อง IoT ขึ้น แนวคิดของ IoT พัฒนาเป็นลำดับจนเกิดโมเมนตัมในปี 19993 (2542) โดยเป็นความคิดในเรื่องการสื่อสารชนิดจากอุปกรณ์ถึงอุปกรณ์ (Device to Device: D2D) เช่น ตู้เย็นถึงมือถือ มือถือถึงเครื่องปรับอากาศ เครื่องจักรถึงเครื่องจักร ฯลฯ IoT ได้รับความนิยมมากขึ้นเป็นลำดับ ในตอนแรกคิดว่าการสื่อสารถึงกันผ่าน Radio-frequency identification (RFID) เป็นเงื่อนไขสำคัญของ IoT โดยคิดว่าถ้าทุกสิ่งของและมนุษย์ทุกคนมี ID (identification) แล้วคอมพิวเตอร์ก็สามารถจัดการได้เกือบทุกเรื่อง

2.2 มาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Systems: ISO 27001:2013)

ความก้าวหน้าของเทคโนโลยีสารสนเทศที่เพิ่มมากขึ้น ส่งผลให้ความต้องการในการดูแลความมั่นคงปลอดภัยของสารสนเทศเพิ่มสูงขึ้นด้วย องค์กรต่าง ๆ ทั้งภาครัฐและภาคเอกชนต่างก็ให้ความสำคัญอย่างมากต่อการพัฒนาระบบเพื่อการดูแลรักษาความมั่นคงปลอดภัยของสารสนเทศขององค์กร มีการพัฒนามาตรฐานเกี่ยวกับการดูแลรักษาความมั่นคงปลอดภัยสารสนเทศออกมาอย่างต่อเนื่อง เพื่อป้องกันความเสียหายที่จะเกิดขึ้นจากภัยคุกคามในรูปแบบต่าง ๆ ที่มีต่อระบบสารสนเทศขององค์กร ซึ่งนับวันจะทวีความรุนแรง และท้าทายต่อผู้บริหารองค์กรที่รับผิดชอบในการดูแลระบบ เป็นอย่างมาก

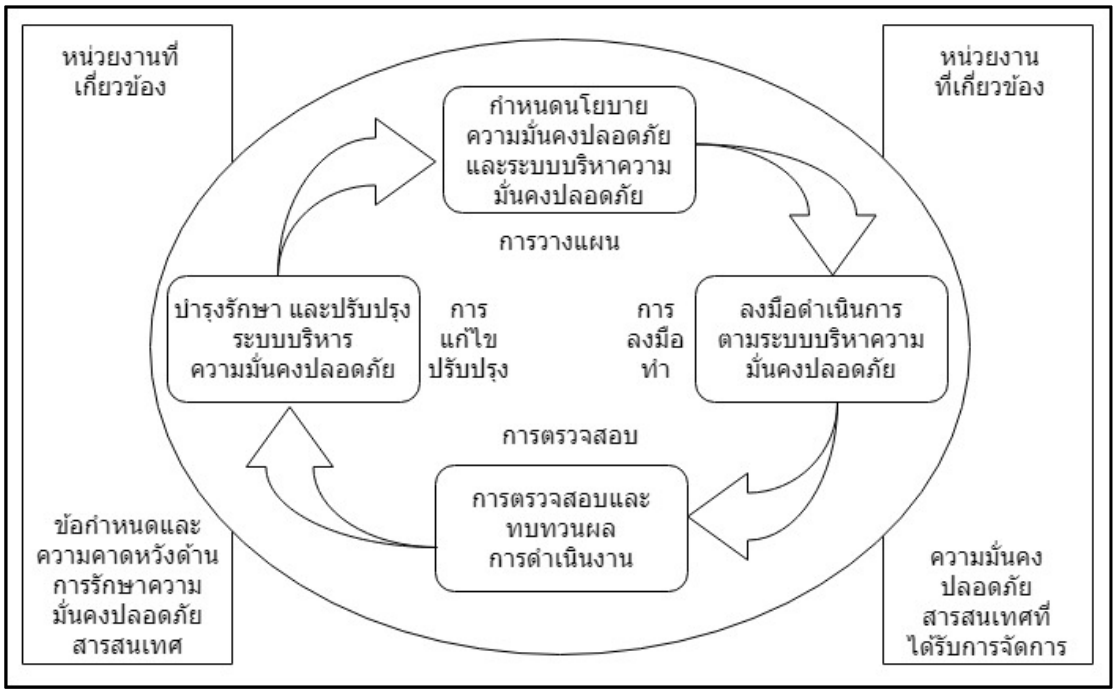
มาตรฐาน ISO/IEC 27001 เป็นมาตรฐานที่พัฒนาขึ้นโดย ISO (International Organization for Standardization) โดยเป็นข้อกำหนดสำหรับการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System, ITSM) เพื่อสร้างความมั่นใจถึงความมีประสิทธิผลและประสิทธิภาพของความมั่นคงปลอดภัยสารสนเทศขององค์กร รวมถึงการดำเนินการที่สอดคล้องตามข้อกำหนดด้านระบบความมั่นคงปลอดภัยทั้งของลูกค้า ข้อกฎหมาย และระเบียบข้อบังคับต่าง ๆ ที่เกี่ยวข้องด้วย

นอกจากมาตรฐาน ISO/IEC 27001 แล้ว ยังได้มีการพัฒนามาตรฐานขึ้นมาอีกฉบับหนึ่งคือ มาตรฐาน ISO/IEC 17799 (Information technology – Security techniques – Code of Practices for Information Security Management) ซึ่งเป็นมาตรฐานที่ระบุถึงแนวปฏิบัติสำหรับการประเมินและจัดการความเสี่ยง รวมถึงแนวทางในการควบคุม ตามมาตรฐาน ISO/IEC 27001 โดยล่าสุดได้ออกมาเป็นรุ่นที่ 2 (Version 2) แล้วในปี 2005 (ปีเดียวกับมาตรฐาน ISO/IEC 27001)

ข้อกำหนดของมาตรฐาน ISO/IEC 27001 ได้แบ่งเนื้อหาของข้อกำหนดออกเป็น 2 ส่วนประกอบด้วย ส่วนของการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ และส่วนของรายการควบคุม และวัตถุประสงค์ของการควบคุม

2.2.1 แนวทางการบริหารความมั่นคงปลอดภัยสารสนเทศ

ในการบริหารจัดการระบบบริหารความมั่นคงปลอดภัยสารสนเทศ จะขับเคลื่อนผ่านวงจร PDCA (ดังรูป) ซึ่งประกอบด้วย การวางแผน (Plan) การลงมือทำ (Do) การตรวจสอบ (Check) และการปรับปรุงแก้ไข (Act) ดังภาพประกอบที่ 2.2



ภาพประกอบที่ 2.2 วงจร PDCA สำหรับการรักษาความมั่นคงปลอดภัยสารสนเทศ

2.2.1.1 การวางแผน

ในขั้นตอนของการวางแผนระบบการบริหารความมั่นคงปลอดภัยสารสนเทศ จะประกอบด้วยขั้นตอนต่าง ๆ ดังนี้

(1.) การกำหนดขอบเขต (Scope) ของระบบ โดยคำนึงถึงลักษณะทางธุรกิจ องค์กร สถานที่ ทรัพย์สิน และเทคโนโลยี รวมถึงรายละเอียดและเหตุผลของสิ่งที่ไม่นำมารวมไว้ในขอบเขตของระบบด้วย

(2.) การกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศ (Information security management system policy) โดยที่นโยบายจะต้อง

(2.1) เป็นกรอบในการจัดทำวัตถุประสงค์ (Objectives) รวมถึงทิศทางและหลักการในการดำเนินการเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ

(2.2) คำนึงถึงข้อกำหนดทางธุรกิจและกฎหมาย รวมถึงข้อบังคับตามสัญญาที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ

(2.3) สอดคล้องกับการบริหารความเสี่ยงเชิงกลยุทธ์ขององค์กร

(2.4) กำหนดเกณฑ์ที่จะใช้ในการประเมินความเสี่ยง และ

(2.5) ได้รับการอนุมัติโดยฝ่ายบริหาร

(3.) การกำหนดแนวทางในการประเมินความเสี่ยงสำหรับองค์กรที่เหมาะสมกับ ISMS และความมั่นคงปลอดภัยสารสนเทศทางธุรกิจ รวมถึงข้อกำหนดทางกฎหมายที่เกี่ยวข้อง

(4.) การระบุความเสี่ยง ซึ่งประกอบด้วย

(4.1) การระบุทรัพย์สินภายในขอบเขตของ ISMS และเจ้าของทรัพย์สินนั้น ๆ

(4.2) การระบุภัยคุกคามที่มีต่อทรัพย์สิน

(4.3) การระบุจุดอ่อนที่ทำให้ภัยคุกคามมีผลกับทรัพย์สิน

(4.4) การระบุถึงผลกระทบที่มีต่อการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้ของทรัพย์สิน

(5.) การวิเคราะห์และประเมินความเสี่ยง โดย

(5.1) การประเมินถึงผลกระทบทางธุรกิจ ซึ่งเกิดจากความล้มเหลวในความมั่นคงปลอดภัย โดยคำนึงถึงความสูญเสียในการรักษาความลับ ความสมบูรณ์หรือความพร้อมของทรัพย์สิน

(5.2) การประเมินถึงโอกาสในการเกิดขึ้นของความล้มเหลวที่มีต่อความมั่นคงปลอดภัย

(5.3) การคำนวณระดับของความเสี่ยง

(5.4) การพิจารณาความสามารถในการยอมรับความเสี่ยง หรือความจำเป็นในการจัดการกับความเสี่ยง โดยใช้เกณฑ์การยอมรับความเสี่ยงที่กำหนดขึ้น

(6.) การกำหนดและประเมินแนวทางในการจัดการความเสี่ยง โดยแนวทางที่ใช้ในการจัดการความเสี่ยง จะประกอบด้วย

(6.1) การกำหนดมาตรการควบคุมที่เหมาะสม

(6.2) การยอมรับความเสี่ยงที่เกิดขึ้น

(6.3) การหลีกเลี่ยงความเสี่ยง และ

(6.4) การโอนย้ายความเสี่ยงไปยังหน่วยงานอื่น ๆ เช่น การประกันภัย

(7.) การคัดเลือกรายการควบคุม และวัตถุประสงค์การควบคุมสำหรับการจัดการความเสี่ยง โดยในขั้นตอนนี้จะเป็นการคัดเลือกหัวข้อการควบคุม และวัตถุประสงค์การควบคุม รวมถึงการนำไปปฏิบัติเพื่อให้สอดคล้องกับแนวทางที่กำหนดจากการประเมิน และกระบวนการจัดการความเสี่ยง โดยการคัดเลือกจะพิจารณาถึงเกณฑ์การยอมรับความเสี่ยง รวมถึงข้อกำหนดทางกฎหมาย และข้อสัญญาต่าง ๆ

(8.) การอนุมัติความเสี่ยงที่เหลืออยู่โดยผู้บริหารระดับสูงขององค์กร

(9.) การอนุมัติโดยผู้บริหารในการดำเนินการ ISMS

(10.) การจัดเตรียมเอกสารแสดงการประยุกต์ใช้งาน หรือ Statement of Applicability (SOA) โดยเอกสาร SOA จะเป็นเอกสารที่อธิบายถึงรายการของหัวข้อควบคุม (Control) และวัตถุประสงค์การควบคุม (Control Objectives ที่ได้เลือกไว้ และเหตุผลของการเลือก รวมถึงหัวข้อควบคุมและวัตถุประสงค์ควบคุมที่มีการดำเนินการอยู่ในปัจจุบัน หรือที่เรียกว่า Base line control ในกรณีที่หัวข้อการควบคุมใดที่ระบุว่าจะไม่มีการดำเนินการ จะต้องมีการระบุถึงเหตุผลของการยกเว้นไว้ด้วย

2.2.1.2 การลงมือทำ

ในขั้นตอนของการลงมือทำจะประกอบด้วย

(1.) การจัดทำแผนการจัดการความเสี่ยง โดยระบุรายละเอียดของการดำเนินงาน ทรัพยากรที่ต้องการ ความรับผิดชอบและลำดับความสำคัญในการดำเนินงาน สำหรับการจัดการกับความเสี่ยงที่มีต่อความมั่นคงปลอดภัยสารสนเทศ

(2.) การดำเนินการตามแผนการจัดการความเสี่ยง เพื่อให้บรรลุตามวัตถุประสงค์การควบคุมที่ได้กำหนดไว้ รวมถึงการพิจารณาจัดสรรเงินทุนและกำหนดหน้าที่ความรับผิดชอบในการดำเนินการด้วย

(3.) การดำเนินการตามการควบคุมที่ได้กำหนดไว้ เพื่อให้ได้ตามวัตถุประสงค์การควบคุม

(4.) การกำหนดแนวทางในการวัดความมีประสิทธิผลของการควบคุม หรือกลุ่มการควบคุมที่ได้กำหนด

(5.) การจัดฝึกอบรมและการสร้างการรับรู้ขึ้นภายในองค์กร

(6.) การบริหารงาน ISMS

(7.) การจัดการทรัพยากรสำหรับ ISMS

(8.) การดำเนินงานตามวิธีการปฏิบัติงาน และการควบคุมอื่น ๆ เพื่อให้สามารถตรวจสอบเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัย และการตอบสนองต่อเหตุการณ์นั้น ๆ

2.2.1.3 การตรวจสอบ

องค์กรจะต้องมีการดำเนินการต่าง ๆ ประกอบด้วย

(1.) การดำเนินการเฝ้าติดตาม และทบทวนวิธีการปฏิบัติงาน และการควบคุมต่าง ๆ เพื่อ

(1.1) ตรวจจับความผิดพลาดของผลลัพธ์ที่ได้จากการประมวลผล

(1.2) ระบุถึงการละเมิดความมั่นคงปลอดภัยและเหตุการณ์ต่าง ๆ ที่เกิดขึ้น

(1.3) ช่วยให้ฝ่ายบริหารสามารถระบุถึงการดำเนินการความมั่นคงที่ได้มอบหมายให้บุคลากรต่าง ๆ เป็นไปตามที่คาดหมายไว้

(1.4) ช่วยในการตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยโดยการใช้ดัชนีวัดที่เหมาะสม

(1.5) พิจารณาถึงความมีประสิทธิผลในการดำเนินการเพื่อแก้ไขการละเมิดความมั่นคงปลอดภัย

(2.) การดำเนินการทบทวนความมีประสิทธิผลของ ISMS อย่างสม่ำเสมอ โดยคำนึงถึงผลของการตรวจประเมินความมั่นคงปลอดภัย (Audit) เหตุการณ์ที่เกิดขึ้น ผลของการวัดความมีประสิทธิผล ข้อเสนอแนะ และข้อมูลแจ้งกลับจากหน่วยงานต่าง ๆ ที่เกี่ยวข้อง

(3.) การวัดความมีประสิทธิผลของการควบคุม เพื่อทวนสอบถึงความสอดคล้องตามข้อกำหนดความมั่นคงปลอดภัย

(4.) ทบทวนการประเมินความเสี่ยงตามแผนที่ได้กำหนดไว้ รวมถึงทบทวนความเสี่ยงที่เหลืออยู่และระดับของความเสี่ยงที่สามารถยอมรับได้ โดยคำนึงถึงการเปลี่ยนแปลงในองค์กร เทคโนโลยี วัตถุประสงค์และกระบวนการทางธุรกิจ ภัยคุกคามที่ระบุไว้ ความมีประสิทธิผลของการควบคุม และเหตุการณ์ภายนอก เช่น การเปลี่ยนแปลงในข้อกฎหมาย ข้อบังคับตามสัญญาที่เปลี่ยนแปลง และการเปลี่ยนแปลงทางสังคม

(5.) การดำเนินการตรวจประเมิน ISMS ภายใน

(6.) การดำเนินการทบทวนโดยฝ่ายบริหาร เพื่อดูแลความเพียงพอของขอบเขต และการดำเนินการปรับปรุงกระบวนการ ISMS

(7.) การปรับปรุงแผนความมั่นคงปลอดภัย โดยคำนึงถึงสิ่งที่พบจากการเฝ้าติดตาม และการทบทวน

(8.) การบันทึกผลการดำเนินการ และเหตุการณ์ที่อาจส่งผลต่อความมีประสิทธิผล หรือผลการดำเนินงานของ ISMS

2.2.1.4 การปรับปรุงแก้ไข

ในขั้นตอนการของการปรับปรุงและแก้ไขระบบ จะประกอบด้วย

(1.) การดำเนินการปรับปรุง ISMS ตามที่ได้กำหนดไว้

(2.) การปฏิบัติการแก้ไขและการป้องกันอย่างเหมาะสม รวมถึงการนำบทเรียนจากประสบการณ์ความมั่นคงปลอดภัยขององค์กรอื่น ๆ และขององค์กรเองมาปรับใช้อย่างเหมาะสม

(3.) การสื่อสารการดำเนินการ และการปรับปรุงไปยังหน่วยงานต่าง ๆ ที่เกี่ยวข้องทั้งหมด

(4.) การดูแลให้มั่นใจว่าการปรับปรุงเป็นไปตามวัตถุประสงค์ที่ได้กำหนดไว้

2.2.2 ข้อกำหนดทางด้านเอกสาร

เอกสารใน ISMS จะประกอบด้วย

2.2.2.1 เอกสารแสดงนโยบาย ISMS และวัตถุประสงค์

2.2.2.2 ขอบเขตของ ISMS

2.2.2.3 วิธีการปฏิบัติงาน และการควบคุมเพื่อสนับสนุนต่อ ISMS

2.2.2.4 คำอธิบายเกี่ยวกับวิธีการประเมินความเสี่ยง

2.2.2.5 รายงานการประเมินความเสี่ยง

2.2.2.6 แผนการจัดการความเสี่ยง

2.2.2.7 เอกสารวิธีการปฏิบัติงานที่จำเป็นสำหรับองค์กร เพื่อให้มั่นใจได้ถึงความมีประสิทธิผลในการวางแผน การดำเนินการ และการควบคุมกระบวนการความมั่นคงปลอดภัยสารสนเทศ และอธิบายถึงแนวทางในการวัดความมีประสิทธิผลของการควบคุม

2.2.2.8 บันทึกที่จำเป็นสำหรับมาตรฐาน

2.2.2.9 เอกสาร Statement of Applicability

2.2.3 การควบคุมเอกสารและบันทึก

เอกสารที่กำหนดโดย ISMS จะต้องได้รับการปกป้องดูแลและควบคุม ทั้งนี้จะต้องมีการจัดทำเอกสารระเบียบการปฏิบัติงานสำหรับการควบคุมเอกสาร โดยระบุถึง

2.2.3.1 การอนุมัติเอกสารก่อนนำไปใช้งาน

2.2.3.2 การทบทวน และปรับปรุงเอกสารให้ทันสมัย รวมถึงมีการอนุมัติซ้ำ

2.2.3.3 การดูแลการเปลี่ยนแปลง และสถานะล่าสุดของเอกสาร

2.2.3.4 การดูแลให้เอกสารฉบับที่เกี่ยวข้องอยู่ ณ จุดใช้งาน

2.2.3.5 เอกสารจะต้องสามารถอ่าน และทำความเข้าใจได้ง่าย

2.2.3.6 การดูแลให้เอกสารพร้อมสำหรับผู้ที่ต้องการใช้งาน รวมถึงมีการแจกจ่าย จัดเก็บ และทำลายให้สอดคล้องตามวิธีการปฏิบัติงานที่กำหนด

2.2.3.7 การระบุอย่างชัดเจนถึงเอกสารจากภายนอกที่มีการนำมาใช้งาน

2.2.3.8 การควบคุมการแจกจ่ายเอกสาร

2.2.3.9 การป้องกันการใช้งานเอกสารที่ยกเลิกแล้ว

2.2.3.10 การชี้บ่งอย่างเหมาะสมกรณีมีการนำเอกสารที่ยกเลิกแล้วกลับมาใช้งาน

ในส่วนของบันทึก จะต้องมีการจัดเก็บและดูแลรักษา เพื่อเป็นหลักฐานแสดงถึงความสอดคล้องตามข้อกำหนด และความมีประสิทธิผลของการดำเนินการ ISMS ทั้งนี้บันทึกต่าง ๆ จะต้องได้รับการปกป้องดูแลและควบคุม โดยจะต้องคำนึงถึงข้อกำหนดทางกฎหมายที่เกี่ยวข้องและข้อบังคับตามสัญญาด้วย นอกจากนั้น บันทึกต่าง ๆ จะต้องอ่าน และเข้าใจได้ง่ายมีการระบุอย่างชัดเจน และสามารถนำมาใช้งานได้โดยง่ายด้วย แนวทางในการควบคุมจะต้องมีการจัดทำเป็นเอกสารระเบียบการปฏิบัติงานไว้อย่างชัดเจน โดยเนื้อหาจะต้องครอบคลุมถึงการระบุ การจัดเก็บ การปกป้องดูแลรักษา การนำมาใช้งาน ระยะเวลาในการจัดเก็บ และการทำลายบันทึกต่าง ๆ

2.2.4 ความรับผิดชอบของฝ่ายบริหาร

ผู้บริหารระดับสูงขององค์กร จะต้องแสดงให้เห็นถึงความมุ่งมั่นต่อการจัดทำ การนำไปปฏิบัติ การปฏิบัติการ การเฝ้าติดตาม การทบทวน การบำรุงรักษา และการปรับปรุง ISMS โดยการ

2.2.4.1 จัดทำนโยบาย ISMS

2.2.4.2 การดูแลให้มีการจัดทำวัตถุประสงค์ของ ISMS

2.2.4.3 การกำหนดบทบาท หน้าที่ความรับผิดชอบสำหรับการดูแลความมั่นคงปลอดภัยสารสนเทศ

2.2.4.4 การสื่อสารถึงความสำคัญของการดำเนินการตามนโยบาย และวัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศ

2.2.4.5 การจัดให้มีทรัพยากรอย่างเพียงพอ สำหรับการจัดทำ การนำไปปฏิบัติ การดำเนินงาน การเฝ้าติดตาม การทบทวน การดูแลรักษา และการปรับปรุง ISMS

2.2.4.6 การตัดสินใจเกี่ยวกับเกณฑ์การยอมรับ และระดับของความเสี่ยงที่สามารถยอมรับได้

2.2.4.7 การดูแลให้มีการตรวจประเมินภายใน (Internal ISMS Audit)

2.2.4.8 การดำเนินการทบทวนโดยฝ่ายบริหาร

2.2.5 การจัดสรรทรัพยากร

องค์กรจะต้องมีการพิจารณา และจัดสรรทรัพยากรอย่างเพียงพอ สำหรับ

2.2.5.1 การจัดทำ การนำไปปฏิบัติ การดำเนินการ การเฝ้าติดตาม การทบทวน การดูแลรักษา และการปรับปรุง ISMS

2.2.5.2 การดูแลให้วิธีการปฏิบัติงานเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ สามารถสนับสนุนต่อความต้องการทางธุรกิจ

2.2.5.3 การระบุข้อกำหนดทางกฎหมาย และข้อบังคับด้านความมั่งคงปลอดภัยตามสัญญา

2.2.5.4 การดูแลความเพียงพอของความมั่นคงปลอดภัย โดยการใช้มาตรการที่ถูกต้อง

2.2.5.5 การทบทวน และการดำเนินการจากผลการทบทวน

2.2.5.6 การปรับปรุงความมีประสิทธิผลของ ISMS

2.2.6 การฝึกอบรม การรับรู้ และความสามารถ

บุคลากรที่ได้รับมอบหมายหน้าที่ตามที่กำหนดใน ISMS จะต้องมีความสามารถอย่างเพียงพอ โดยที่จะต้อง

2.2.6.1 มีการกำหนดความสามารถที่จำเป็นสำหรับการดำเนินงานที่มีผลกระทบต่อ ISMS

2.2.6.2 จัดให้มีการฝึกอบรมหรือการดำเนินตามความเหมาะสม เพื่อตอบสนองต่อความจำเป็นดังกล่าว

2.2.6.3 มีการประเมินความมีประสิทธิผลของการดำเนินงานที่เกิดขึ้น

2.2.6.4 ดูแลบันทึกเกี่ยวกับการศึกษา การฝึกอบรม ทักษะ ประสบการณ์ และคุณสมบัติ

นอกจากนั้น องค์กรจะต้องดูแลให้มั่นใจว่าบุคลากรที่เกี่ยวข้องทั้งหมด รับรู้ถึงความสำคัญและความเกี่ยวข้องที่มีต่อความมั่นคงปลอดภัยสารสนเทศ และการมีส่วนร่วมต่อความสำเร็จของวัตถุ ประสงค์ ISMS

2.2.7 การตรวจประเมินภายใน

กระบวนการหนึ่งที่สำคัญที่จะช่วยให้มั่นใจได้ถึงความเพียงพอ ความเหมาะสม และความสอดคล้องตามข้อกำหนดของ ISMS รวมถึงเป็นช่องทางในการหาโอกาสในการปรับปรุงระบบให้ดียิ่งขึ้น ได้แก่ การตรวจประเมินภายใน หรือ Internal ISMS Audit โดยองค์กรจะต้องจัดให้มีการตรวจประเมินภายในตามแผนการตรวจที่กำหนดไว้ ทั้งนี้การตรวจประเมินจะมีเป้าหมายเพื่อพิจารณาว่าวัตถุประสงค์การควบคุม การควบคุม กระบวนการ และวิธีการปฏิบัติงานของ ISMS

2.2.7.1 สอดคล้องตามข้อกำหนดของมาตรฐาน ISO/IEC 27001 รวมถึงข้อกำหนดทางกฎหมายที่เกี่ยวข้อง

2.2.7.2 สอดคล้องตามข้อกำหนดความมั่นคงปลอดภัยสารสนเทศที่ได้กำหนดไว้

2.2.7.3 มีการดำเนินการ และดูแลรักษาอย่างมีประสิทธิผล

2.2.7.4 เป็นไปตามที่ได้คาดหมายไว้

ทั้งนี้จะต้องมีการจัดทำโปรแกรมการตรวจประเมินภายใน โดยคำนึงถึงสถานะและความสำคัญของกระบวนการ และหน่วยงานที่จะทำการตรวจ รวมถึงผลการตรวจที่ผ่านมา ทั้งนี้จะต้องมีการกำหนดเกณฑ์ในการตรวจประเมิน ขอบเขตความถี่ และวิธีการที่ใช้ในการตรวจ รวมถึงการคัดเลือกผู้ตรวจประเมิน และการดำเนินการตรวจประเมินด้วยความยุติธรรม และเสมอภาค ทั้งนี้ผู้ตรวจประเมินจะต้องไม่ตรวจในหน่วยงานของตนเอง

ผู้รับผิดชอบในหน่วยงานที่ถูกตรวจ จะต้องดำเนินการเพื่อขจัดความไม่เป็นไปตามข้อกำหนดที่ตรวจพบโดยไม่ให้เกิดความล่าช้าขึ้น รวมถึงจะต้องมีการติดตามผลการดำเนินการแก้ไข และมีการรายงานผลการติดตามด้วย

2.2.8 การทบทวนโดยฝ่ายบริหาร

อย่างที่ได้อธิบายไปแล้วในบทบาทของฝ่ายบริหาร ที่จะต้องจัดให้มีการทบทวนโดยฝ่ายบริหาร ตามช่วงเวลาที่ได้วางแผนไว้ เพื่อให้มั่นใจถึงความเหมาะสม ความเพียงพอ และความมีประสิทธิผลของระบบอย่างต่อเนื่อง โดยการทบทวนจะรวมไปถึงการประเมินโอกาสในการปรับปรุงระบบ และความจำเป็นในการเปลี่ยนแปลง ISMS ทั้งในส่วนของนโยบายความมั่นคงปลอดภัย และวัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศ ผลของการทบทวนจะต้องมีการจัดทำเป็นเอกสารอย่างชัดเจน และได้รับการควบคุมตามข้อกำหนดการควบคุมบันทึกด้วย

สิ่งที่จะต้องนำมาทบทวน ประกอบด้วย

2.2.8.1 ผลของการตรวจประเมินและการทบทวน ISMS

2.2.8.2 การแจ้งข้อมูลกลับจากหน่วยงานต่าง ๆ ที่เกี่ยวข้อง

2.2.8.3 เทคนิค ผลิตภัณฑ์ หรือวิธีการปฏิบัติงาน ซึ่งใช้ในการปรับปรุงผลการดำเนินงานและความมีประสิทธิผลของ ISMS

2.2.8.4 สถานะของการปฏิบัติการแก้ไข และการป้องกัน

2.2.8.5 จุดอ่อนหรือภัยคุกคาม ที่ยังไม่นำมาประเมินความเสี่ยง

2.2.8.6 ผลของการวัดความมีประสิทธิผล

2.2.8.7 การติดตามความคืบหน้าจากการทบทวนโดยฝ่ายบริหารที่ผ่านมา

2.2.8.8 การเปลี่ยนแปลงที่มีผลกระทบต่อ ISMS และ

2.2.8.9 ข้อเสนอแนะเพื่อการปรับปรุงงาน

ผลลัพธ์ที่ได้จากการทบทวนโดยฝ่ายบริหาร จะเป็นการตัดสินใจ และการดำเนินการในส่วนที่เกี่ยวกับ

2.2.8.10 การปรับปรุงความมีประสิทธิผลของ ISMS

2.2.8.11 การปรับปรุงการประเมินความเสี่ยง และแผนการจัดการความเสี่ยง

2.2.8.12 การปรับเปลี่ยนวิธีการปฏิบัติงาน และการควบคุมที่มีผลกระทบต่อความมั่นคงปลอดภัย เพื่อตอบสนองต่อเหตุการณ์ทั้งภายในและภายนอกซึ่งมีผลกระทบต่อ ISMS เช่น การเปลี่ยนแปลงในข้อกำหนดทางธุรกิจ ข้อกำหนดความมั่นคงปลอดภัย กระบวนการทางธุรกิจที่มีผลกระทบต่อข้อกำหนดทางธุรกิจ ข้อกำหนดทางกฎหมาย ข้อบังคับตามสัญญา และระดับของความเสี่ยงหรือเกณฑ์การยอมรับความเสี่ยง

2.2.8.13 ทรัพยากรที่จำเป็น

2.2.8.14 การปรับปรุงแนวทางในการสร้างความมีประสิทธิผลของการควบคุม

2.2.9 การปรับปรุงอย่างต่อเนื่อง

ในการปรับปรุงความมีประสิทธิผลอย่างต่อเนื่องของ ISMS จะต้องมีการดำเนินการโดยพิจารณาจากนโยบายความมั่นคงปลอดภัยสารสนเทศ วัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศ ผลการตรวจประเมิน การวิเคราะห์เหตุการณ์ที่เกิดขึ้น การปฏิบัติการแก้ไขและการป้องกัน และการทบทวนโดยฝ่ายบริหาร

2.2.10 การปฏิบัติการแก้ไข

ในกรณีที่เกิดความไม่สอดคล้องตามข้อกำหนดของ ISMS ขึ้น องค์กรจะต้องมีการดำเนินการเพื่อขจัดสาเหตุของความไม่สอดคล้องนั้น ๆ เพื่อป้องกันการเกิดขึ้นซ้ำ ทั้งนี้จะต้องมีการจัดทำเอกสารระเบียบวิธีการปฏิบัติงาน ที่ระบุถึง

2.2.10.1 การระบุความไม่สอดคล้องตามข้อกำหนด

2.2.10.2 การพิจารณาสาเหตุของความไม่สอดคล้องตามข้อกำหนด

2.2.10.3 การประเมินถึงความจำเป็นในการดำเนินการ เพื่อให้มั่นใจได้ว่าความไม่สอดคล้องตามข้อกำหนดจะไม่เกิดขึ้นซ้ำ

2.2.10.4 การดำเนินการปฏิบัติการแก้ไข

2.2.10.5 การบันทึกผลของการดำเนินการ

2.2.10.6 การทบทวนการปฏิบัติการแก้ไข

2.2.11 การปฏิบัติการป้องกัน

องค์กรจะต้องมีการกำหนดมาตรการดำเนินการ เพื่อขจัดสาเหตุของความไม่สอดคล้องตามข้อกำหนดของ ISMS ที่อาจจะเกิดขึ้นด้วย เพื่อป้องกันไม่ให้ความไม่สอดคล้องตามข้อกำหนดนั้นสามารถเกิดขึ้นได้ ทั้งนี้จะต้องมีการจัดทำเอกสารระเบียบการปฏิบัติงาน ที่ระบุถึง

2.2.11.1 การระบุถึงความไม่สอดคล้องตามข้อกำหนดที่อาจจะเกิดขึ้น รวมถึงสาเหตุ

2.2.11.2 การประเมินถึงความจำเป็นในการดำเนินการ เพื่อป้องกันการเกิดขึ้นของความไม่สอดคล้องตามข้อกำหนด

2.2.11.3 การดำเนินการปฏิบัติการป้องกัน

2.2.11.4 การบันทึกผลการดำเนินการ

2.2.11.5 การทบทวนการปฏิบัติการป้องกัน

นอกจากนั้น องค์กรยังต้องมีการระบุถึงความเสี่ยงที่เปลี่ยนแปลงไป และดำเนินการป้องกันโดยคำนึงถึงความเสี่ยงที่เปลี่ยนแปลงไปอย่างมีนัยสำคัญด้วย

นอกเหนือจากข้อกำหนดเกี่ยวกับระบบการบริหารความมั่นคงปลอดภัยแล้ว ในมาตรฐาน ISO/IEC 27001 ยังมีการระบุข้อกำหนดเฉพาะ (Specific Requirements) ในส่วนของรายการควบคุม (Controls) และวัตถุประสงค์การควบคุม (Control Objectives) ซึ่งจะกำหนดรายการที่เกี่ยวกับความมั่นคงปลอดภัย (Security) ที่จะต้องดำเนินการควบคุม

ในขั้นตอนของการวางแผนระบบบริหารความมั่นคงปลอดภัย (Planning) ได้ระบุให้มีการกำหนดรายการควบคุม (Controls) และวัตถุประสงค์การควบคุม (Control Objectives) ที่เหมาะสมกับองค์กร โดยรายการควบคุมที่กำหนด จะต้องมีการระบุไว้อย่างชัดเจนใน Statement of Applicability (SOA) ด้วย

2.2.12 รายการควบคุม

2.2.12.1 นโยบายความมั่นคงปลอดภัย

ในข้อกำหนดได้ระบุให้มีการจัดทำนโยบายความมั่นคงปลอดภัย (Information Security Policy) โดยจะต้องได้รับการอนุมัติจากผู้บริหารระดับสูง มีการจัดพิมพ์เผยแพร่ และมีการสื่อสารไปยังพนักงานทุกคน รวมถึงหน่วยงานภายนอกอื่น ๆ ที่เกี่ยวข้อง นอกจากนั้น ยังต้องมีการทบทวนถึงความเหมาะสม ความเพียงพอ และความมีประสิทธิผลของนโยบายอย่างต่อเนื่องด้วย

2.2.12.2 การจัดองค์กรในการดูแลความมั่นคงปลอดภัย

ผู้บริหารระดับสูงขององค์กร จะต้องให้การสนับสนุนอย่างเต็มที่ต่อการรักษาความมั่นคงปลอดภัย โดยการกำหนดทิศทางอย่างชัดเจน มีการมอบหมายงาน และสร้างการรับรู้ถึงความรับผิดชอบที่มีต่อความมั่นคงปลอดภัยสารสนเทศ รวมถึงการจัดให้มีรูปแบบการประสานงานระหว่างหน่วยงานต่าง ๆ ภายในองค์กร เช่น การจัดทำผังโครสร้างการทำงาน (Organization Chart) หรือผังการปฏิบัติงาน (Operation Cart) และการกำหนดหน้าที่ ความรับผิดชอบในส่วนที่เกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศอย่างทั่วถึงด้วย

องค์กรจะต้องมีการกำหนดกระบวนการในการอนุมัติ กรณีที่มีการจัดซื้อหรือจัดหาอุปกรณ์ เครื่องมือ หรือสิ่งอำนวยความสะดวกใหม่ๆ สำหรับการนำมาใช้งาน รวมถึงจะต้องมีการจัดทำข้อตกลงในการดูแลรักษาความลับ (Confidentiality Agreement) กับทุก ๆ ส่วนที่เกี่ยวข้อง นอกจากนั้น จะต้องจัดให้มีการทบทวนองค์ประกอบต่าง ๆ ของการบริหารความมั่นคงปลอดภัยสารสนเทศ เช่น วัตถุประสงค์การควบคุม การควบคุม นโยบาย กระบวนการ และวิธีการปฏิบัติงานสำหรับการรักษาความมั่นคงปลอดภัย ตามแผนงานที่ได้กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญกับการปฏิบัติงานเกิดขึ้น

ในส่วนของหน่วยงานภายนอก จะต้องมีการระบุถึงความเสี่ยงต่าง ๆ ที่เกี่ยวกับหน่วยงานภายนอก ในกรณีที่หน่วยงานเหล่านั้น มีการใช้งานหรือมีความเกี่ยวข้องกับสารสนเทศ หรือ

อุปกรณ์ในการประมวลผลองค์กร จะต้องมีการจัดทำข้อตกลงทางด้านการรักษาความมั่นคงปลอดภัยสารสนเทศกับหน่วยงานเหล่านั้นด้วย

2.2.12.3 การจัดการทรัพย์สิน

คำว่า “ทรัพย์สิน (Asset)” ในมาตรฐาน จะหมายถึงสิ่งใด ๆ ที่มีคุณค่ากับองค์กร ซึ่งจะรวมไปถึงเครื่องมือ อุปกรณ์ ฮาร์ดแวร์ ซอฟต์แวร์ ฐานข้อมูล บุคลากร สาธารณูปโภคต่าง ๆ โดยข้อกำหนดในหัวข้อควบคุมนี้ จะระบุให้ต้องมีการจัดทำบัญชีทรัพย์สินทั้งหมด มีการกำหนดเจ้าของที่รับผิดชอบในการควบคุมการใช้งาน และการรักษาความมั่นคงปลอดภัยของทรัพย์สิน รวมถึงการกำหนดแนวทางในการใช้งานอย่างเหมาะสมด้วย

นอกจากนั้น จะต้องมีการกำหนดแนวทางในการจัดแยกประเภทของสารสนเทศ (Information Classification) โดยพิจารณาจากคุณค่า ข้อกำหนดทางกฎหมาย ความอ่อนไหว และความสำคัญที่มีกับองค์กร จากนั้นให้มีการจัดทำฉลาก (Labeling) เพื่อแสดงสถานะของสารสนเทศ รวมถึงแนวทางในการจัดการตลอดช่วงอายุของสารสนเทศนั้น ๆ

2.2.12.4 ความมั่นคงปลอดภัยเกี่ยวกับบุคลากร

ในข้อกำนดการควบคุมนี้ ได้แบ่งออกเป็น 3 ส่วน ประกอบด้วยก่อนที่จะมีการจ้างงาน ในระหว่างการจ้างงาน และเมื่อยกเลิกการจ้างงาน

ก่อนที่จะมีการจ้างงาน จะต้องมีการกำหนดบทบาท หน้าที่ความรับผิดชอบที่เกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศสำหรับพนักงานทุกคน รวมถึงผู้รับจ้างช่วง และหน่วยงานภายนอก ไว้เป็นเอกสารอย่างชัดเจน โดยจะต้องสอดคล้องนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กรด้วย รวมถึงจะต้องมีการกำหนดแนวทางในการคัดเลือก (Screening) โดยจะต้องมีการตรวจสอบคุณสมบัติของผู้สมัครอย่างละเอียด และมีการกำหนดเงื่อนไขการจ้างงานที่เหมาะสม ครอบคลุมถึงเงื่อนไขในส่วนที่เกี่ยวกับความรับผิดชอบในส่วนของความมั่นคงปลอดภัยสารสนเทศ

ในระหว่างการจ้างงาน พนักงานทุกคน รวมถึงผู้รับจ้างช่วง และหน่วยงานภายนอกที่เกี่ยวข้อง จะต้องปฏิบัติตามนโยบายและวิธีการปฏิบัติงานในการรักษาความมั่นคงปลอดภัยสารสนเทศที่กำหนดขึ้นในองค์กร ทั้งนี้องค์กรจะต้องจัดให้มีการฝึกอบรม และสร้างการรับรู้อย่างเหมาะสมให้กับทุก ๆ คนที่เกี่ยวข้องด้วย นอกจากนั้น ยังต้องกำหนดแนวทางในการลงโทษสำหรับพนักงานที่ไม่ปฏิบัติตามแนวปฏิบัติด้านความมั่นคงปลอดภัยขององค์กร

เมื่อมีการยกเลิกการจ้างงาน องค์กรจะต้องมีการกำหนดผู้รับผิดชอบในการจัดการเมื่อมีการยกเลิกการจ้างงานไว้อย่างชัดเจนด้วย ทั้งนี้พนักงานทุกคน รวมถึงผู้รับจ้างช่วงจะต้องส่งทรัพย์สินทั้งหมดคืนให้กับองค์กร และให้ทำการยกเลิกสิทธิในการเข้าถึงสารสนเทศ หรือสถานที่ปฏิบัติงานที่จะต้องมีการควบคุมทั้งหมด เมื่อได้ยกเลิกการจ้างงานแล้ว

2.2.12.5 ความมั่นคงปลอดภัยทางกายภาพ

จะต้องจัดให้มีรั้วรอบบริเวณ ประตูทางเข้าอาคาร ผนังกั้นหรือแม้แต่โต๊ะของเจ้าหน้าที่ต้อนรับหรือเจ้าหน้าที่รักษาความปลอดภัย เพื่อเป็นการป้องกันและควบคุมการเข้าออกพื้นที่ทำงานหรือพื้นที่จัดเก็บสารสนเทศ ทั้งนี้จะต้องมีการกำหนดแนวทางในการควบคุมการเข้าออกของพื้นที่ต่าง ๆ ด้วย เช่น การใช้บัตรเข้าออก การใช้กล้องวงจรปิด การลงบันทึกการเข้าออก เป็นต้น นอกจากนั้นจะต้องกำหนดให้มีการดูแลความมั่นคงปลอดภัยของทั้งสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวกต่าง ๆ รวมถึงมีการป้องกันผลกระทบจากภัยธรรมชาติ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การก่อการร้าย การประท้วง และอื่น ๆ

สำหรับการปฏิบัติงานในพื้นที่ที่สำคัญ (Secure Areas) จะต้องมีการกำหนดแนวปฏิบัติ (Guideline) สำหรับการปฏิบัติงานในพื้นที่ดังกล่าวอย่างชัดเจนด้วย รวมถึงจะต้องมีการกำหนดพื้นที่ในการรับสินค้าแยกต่างหาก เพื่อป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตสามารถเข้าถึงในพื้นที่ที่สำคัญได้

นอกจากนั้น ข้อกำหนดยังระบุถึงการดูแลความมั่นคงปลอดภัยของเครื่องมือ และอุปกรณ์ต่าง ๆ โดยจะต้องมีการจัดวางอย่างเหมาะสม เพื่อลดความเสี่ยงจากภัยอันตรายต่าง ๆ รวมถึงป้องกันโอกาสที่จะถูกนำไปใช้งานโดยไม่ได้รับอนุญาติและป้องกันความเสียหายที่จะเกิดขึ้นจากความล้มเหลวของอุปกรณ์สนับสนุนต่าง ๆ เช่น ระบบไฟฟ้า ระบบควบคุม อุณหภูมิ ระบบปรับอากาศ เป็นต้น

ในส่วนของสายเคเบิลทั้งสายเคเบิลไฟฟ้า และสายเคเบิลสื่อสาร จะต้องได้รับการปกป้องดูแลจากความเสียหายต่าง ๆ ที่อาจจะเกิดขึ้น รวมถึงจะต้องจัดให้มีการบำรุงรักษา (Maintenance) อุปกรณ์อย่างต่อเนื่อง เพื่อให้มั่นใจได้ถึงความพร้อมใช้ และความสมบูรณ์ต่อการนำมาใช้งาน

ในกรณีที่มีการนำอุปกรณ์ออกไปใช้นอกสถานที่ (Off-Premises) ซึ่งจะมีความเสี่ยงที่แตกต่างจากการใช้งานภายในองค์กร จะต้องมีการกำหนดแนวทางในการดูแลความมั่นคงปลอดภัยในการนำไปใช้งานอย่างเหมาะสมด้วย และเมื่อมีการยกเลิกการใช้งานอุปกรณ์นั้น ๆ แล้ว จะต้อง

ดูแลให้มั่นใจว่าข้อมูล สารสนเทศ หรือซอฟท์แวร์ต่าง ๆ ที่อยู่ในอุปกรณ์ได้รับการกำจัด หรือลบทิ้งจนหมดสิ้น ก่อนที่จะทำการทิ้งหรือกำจัดอุปกรณ์นั้น ๆ

2.2.12.6 การบริหารการสื่อสารและการดำเนินการ

ในข้อกำหนดได้ระบุให้มีการจัดทำเอกสารวิธีการปฏิบัติงานในการดำเนินงาน รวมถึงจะต้องกำหนดให้มีกระบวนบริหารการเปลี่ยนแปลง (Change Management) ที่จะเกิดขึ้นด้วย นอกจากนั้น ยังต้องมีการแบ่งหน้าที่ความรับผิดชอบอย่างชัดเจน เพื่อลดโอกาสในการเข้าถึงระบบโดยไม่ได้รับอนุญาติ หรือมีการใช้งานที่ผิดวัตถุประสงค์ของทรัพย์สินขององค์กร

ทั้งนี้ จะต้องมีการแบ่งแยกกระบวนการออกแบบ ทดสอบ และการใช้งานจริงออกจากกันอย่างชัดเจน เพื่อป้องกันความเสี่ยงจากการใช้งาน รวมถึงการเปลี่ยนแปลงระบบการปฏิบัติงานโดยไม่ได้รับอนุญาติ

ในการให้บริการโดยหน่วยงานภายนอก (Third Party) จะต้องมีควบคุมเพื่อให้มั่นใจว่าหน่วยงานภายนอกนั้น ได้ให้บริการตามที่ได้มีการตกลงกันไว้ รวมถึงยังต้องมีการเฝ้าติดตาม ทบทวน และตรวจประเมิน (Audit) การให้บริการโดยหน่วยงานภายนอกด้วย ในกรณีที่มีการเปลี่ยนแปลงเกิดขึ้น ซึ่งเกี่ยวข้องกับการให้บริการโดยหน่วยงานภายนอก จะต้องมีการทบทวน และปรับปรุงแก้ไขข้อตกลงในการให้บริการด้วย

ข้อกำหนดยังได้ระบุถึงการวางแผนขีดความสามารถ (Capacity Planning) ไว้ด้วย โดยจะต้องมีการติดตามการใช้ทรัพยากร และวางแผนความต้องการที่จะเกิดขึ้นในอนาคต เพื่อให้ระบบมีความเหมาะสมต่อการใช้งาน นอกจากนั้นจะต้องมีการกำหนดเกณฑ์การยอมรับระบบสารสนเทศทั้งที่มีการเปลี่ยนแปลงแก้ไข และที่เป็นระบบใหม่ รวมถึงมีการดำเนินการทดสอบตามเกณฑ์ที่กำหนดก่อนที่จะมีการยอมรับเพื่อนำมาใช้งานต่อไป

นอกจากนั้น ข้อกำหนดยังได้ระบุให้มีมาตรการในการป้องกันโปรแกรมที่ไม่พึงประสงค์ (Malicious Code) หรือไม่หวังดีต่อระบบ ตั้งแต่ การตรวจจับ การป้องกัน และการกู้คืนระบบเมื่อเกิดปัญหาขึ้น ในกรณีของโปรแกรมชนิดเคลื่อนที่ (Mobile Code) จะต้องมีมาตรการเพื่อควบคุมให้เป็นไปตามนโยบายความมั่นคงปลอดภัยด้วย รวมถึงจะต้องจัดให้มีการดำเนินการสำรอง (Back-up) ทั้งข้อมูล และซอฟต์แวร์ รวมถึงมีการทดสอบอย่างสม่ำเสมอ เพื่อให้เป็นไปตามนโยบายการสำรองข้อมูลที่ได้กำหนดไว้

2.2.12.7 การควบคุมการเข้าถึงระบบ

จะต้องมีการกำหนดนโยบายในการเข้าถึงระบบ (Access Control Policy) มีการจัดทำเป็นเอกสารชัดเจน และมีการทบทวนโดยพิจารณาถึงความต้องการทางธุรกิจ และข้อกำหนดความมั่นคงปลอดภัยด้วย

ในการบริหารการเข้าถึงของผู้ใช้งาน (User Access) จะต้องมีการจัดทำแนวทางในการขึ้นทะเบียนของผู้ใช้งาน (User Registration) และการยกเลิกทะเบียนของผู้ใช้งาน เช่น เมื่อลาออกจากองค์กร หรือมีการเปลี่ยนแปลงตำแหน่งหน้าที่งาน ทั้งนี้จะต้องมีมาตรการในการจำกัดและควบคุมสิทธิในการใช้งานระบบ และรหัสผ่านสำหรับผู้ใช้งาน นอกจากนั้น จะต้องจัดให้มีการทบทวนสิทธิในการเข้าถึงระบบของผู้ใช้งานอย่างสม่ำเสมอด้วย

ในการบริหารจัดการ จะต้องมีการกำหนดแนวปฏิบัติที่ดีสำหรับการคัดเลือก และการใช้งานรหัสผ่าน (Password) รวมถึงจะต้องมีการป้องกันไม่ให้มีการใช้งานอุปกรณ์โดยไม่ได้รับอนุญาติด้วย นอกจากนั้น ยังต้องมีการกำหนดนโยบายในการควบคุมการจัดเก็บเอกสาร หรือสื่อที่ใช้บันทึกข้อมูลต่าง ๆ ไว้ในที่ที่ปลอดภัยด้วย

สำหรับการควบคุมการเข้าถึงเครือข่าย (Network Access Control) จะต้องมีการกำหนดนโยบายในการเข้าถึงเครือข่าย โดยต้องระบุอย่างชัดเจนถึงบริการใดที่ผู้ใช้งานสามารถเข้าถึงได้ รวมถึงการแสดงตัวของผู้ใช้งานจากการใช้งานจากภายนอกองค์กร (External Connection) จะต้องมีการกำหนดวิธีการที่เหมาะสมด้วย เช่นเดียวกันกับการแสดงตัวตนสำหรับอุปกรณ์หรือเครื่องมือที่มีการเชื่อมต่อเครือข่ายจากภายนอก นอกจากนั้น ยังต้องมีการควบคุมการเข้าถึงพอร์ตสำหรับการวินิจฉัยและการปรับแต่งระบบ รวมถึงในการพิจารณาเพื่อแบ่งแยกเครือข่าย (Network Segregation) จะพิจารณาตามกลุ่มของบริการสารสนเทศ ผู้ใช้งาน และระบบสารสนเทศ

ทั้งนี้การเชื่อมต่อเครือข่ายจะต้องได้รับการควบคุม โดยมีการจำกัดผู้ใช้งานในการเชื่อมต่อกับเครือข่ายระหว่างองค์กร ให้สอดคล้องกับนโยบายการเข้าถึงระบบ (Access Control Policy) และข้อกำหนดของแอปพลิเคชันที่ใช้ด้วย รวมถึงจะต้องมีการควบคุมเส้นทางของเครือข่าย โดยต้องมีการกำหนดเส้นทางเพื่อให้มั่นใจว่าการเชื่อมต่อคอมพิวเตอร์ และการไหลของสารสนเทศ เป็นไปตามนโยบายการเข้าถึงระบบ (Access Control Policy) ด้วย

ในการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System) จะต้องมีการกำหนดขั้นตอนการปฏิบัติงานที่เหมาะสมในการเข้าถึงหรือการใช้งานระบบปฏิบัติการ โดยผู้ใช้งานทั้งหมดจะต้องมีการระบุตัวตน (Unique Identifier, User ID) ก่อนใช้งานด้วย รวมถึงจะต้องมีระบบในการจัดการ

รหัสผ่านอย่างมีคุณภาพ ส่วนการใช้โปรแกรมประเภทยูทิลิตี้ (Utility Program) จะต้องมีการจำกัดและควบคุมการใช้งานโปรแกรมดังกล่าว เพื่อป้องกันการละเมิดการควบคุมระบบและแอปพลิเคชันที่กำหนดไว้

นอกจากนั้นยังต้องมีการควบคุมเวลาในการใช้งานระบบสารสนเทศ (Session Time-out) โดยจะต้องมีการตัดหรือหยุดการใช้งาน เมื่อผู้ใช้งานไม่ได้มีการใช้ระบบมาเป็นระยะเวลาหนึ่ง รวมถึงจะต้องมีการกำหนดเวลาในการเชื่อมต่อเครือข่าย (Connection Time) สำหรับแอปพลิเคชันที่มีความเสี่ยงสูงด้วย

ส่วนการควบคุมการเข้าถึงแอปพลิเคชั่น และสารสนเทศ จะต้องมีการจำกัดการใช้งานสำหรับผู้ใช้งานและเจ้าหน้าที่สนับสนุนให้สอดคล้องตามนโยบายควบคุมการเข้าถึงระบบ (Access Control Policy) รวมถึงจะต้องมีการแยกแยะสารสนเทศที่มีความสำคัญอย่างมากออกไว้ต่างหากด้วย

ในกรณีของอุปกรณ์ประเภทพกพา หรือการปฏิบัติงานจากภายนอกองค์กร จะต้องมีการกำหนดนโยบายในการควบคุมอย่างเหมาะสม เพื่อป้องกันความเสี่ยงจากการใช้งานอุปกรณ์แบบพกพา นอกจากนั้น จะต้องมีการกำหนดนโยบาย แผนงาน และวิธีการปฏิบัติงานที่จำเป็นด้วยสำหรับการปฏิบัติจากภายนอกองค์กร (Teleworking)

2.2.12.8 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

องค์กรจะต้องจัดให้มีการวิเคราะห์ และระบุถึงข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศใหม่ หรือเมื่อมีการปรับปรุงระบบที่มีอยู่ในปัจจุบัน

ในส่วนของการประมวลผลในแอปพลิเคชัน จะต้องมีการทวนสอบถึงความถูกต้องและความเหมาะสมของข้อมูลที่นำมาใช้ในการประมวลผลโดยแอปพลิเคชัน รวมถึงการทวนสอบความถูกต้องของข้อมูลในระหว่างการประมวลผล เพื่อป้องกันความผิดพลาด หรือมีการเปลี่ยนแปลงแก้ไขเกิดขึ้น นอกจากนั้น จะต้องมีการตรวจสอบความถูกต้องของข้อความ (Message) ที่แสดงในแอปพลิเคชัน รวมถึงในส่วนของข้อมูลที่ได้จากการประมวลผลของแอปพลิเคชัน จะต้องมีการทวนสอบความถูกต้องและมีความเหมาะสมด้วย

ในการควบคุมการเข้ารหัสข้อมูล (Cryptographic) จะต้องมีการกำหนดนโยบายในการควบคุมเข้ารหัสข้อมูล และมีการนำไปใช้ทั่วทั้งองค์กร รวมถึงจะต้องมีมาตรการในการจัดการกับกุญแจที่ใช้ในการเข้ารหัสหรือถอดรหัสข้อมูล โดยจะใช้ร่วมกันกับเทคนิคที่ใช้ในการเข้ารหัสข้อมูล

สำหรับความมั่นคงปลอดภัยของแฟ้มระบบ (System Files) จะต้องมีการกำหนดวิธีการปฏิบัติงานในการควบคุมการติดตั้งซอฟต์แวร์ลงในระบบการปฏิบัติการ (Operational System) รวมถึงข้อมูลที่ใช้ในการทดสอบ จะต้องมีการคัดเลือกอย่างระมัดระวัง มีการควบคุม และปกป้องดูแล รวมถึงจะต้องมีการควบคุมการเข้าถึงซอร์สโค๊ดของระบบด้วย

ในกระบวนการพัฒนาระบบ และกระบวนการสนับสนุน จะต้องมีการจัดทำขั้นตอนการปฏิบัติงานในการควบคุมการเปลี่ยนแปลงระบบอย่างเป็นทางการ ทั้งนี้เมื่อระบบมีการเปลี่ยนแปลง จะต้องมีการทบทวนและทดสอบแอปพลิเคชันเพื่อให้มั่นใจได้ว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงานขององค์กร หรือต่อความมั่นคงปลอดภัยของระบบ นอกจากนั้น จะต้องมีการจำกัดการเปลี่ยนแปลงแก้ไขซอฟต์แวร์จากผู้ผลิต และถ้าจะต้องมีการเปลี่ยนแปลง จะต้องได้รับการควบคุมอย่างเข็มงวด รวมถึงจะต้องมีการป้องกันการรั่วไหลของสารสนเทศขององค์กร ในกรณีที่การพัฒนาซอฟท์แวร์ดำเนินการโดยหน่วยงานภายนอก จะต้องมีการกำหนดมาตรการในการดำเนินการควบคุม และตรวจสอบอย่างชัดเจนด้วย

นอกจากนั้น จะต้องมีการกำหนดมาตรการในการจัดการกับช่องโหว่ หรือจุดอ่อนของระบบ โดยจะต้องมีการติดตามข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิคของระบบสารสนเทศอย่างต่อเนื่อง เพื่อทำการประเมินโอกาสที่จะเกิดขึ้น และกำหนดมาตรการที่เหมาะสมในการจัดการกับความเสี่ยงนั้น ๆ

2.2.12.9 การจัดการเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ

เหตุการณ์ต่าง ๆ ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ (Information Security Events) จะต้องมีการรายงานผ่านช่องทางการรายงานอย่างเหมาะสมด้วยความรวดเร็วเท่าที่เป็นไปได้ นอกจากนั้นพนักงานทุกคน ผู้รับจ้างช่วง รวมถึงหน่วยงานภายนอก จะต้องทำการบันทึก และรายงานถึงจุดอ่อนเกี่ยวกับความมั่นคงปลอดภัยของระบบหรือบริการ ที่สังเกตุพบหรือสงสัยว่าจะเกิดขึ้นในระบบ

ทั้งนี้ องค์กรจะต้องมีการกำหนดบทบาท หน้าที่ความรับผิดชอบที่ชัดเจน ในการจัดการกับเหตุการณ์ที่เกิดขึ้นด้วยความรวดเร็ว และมีประสิทธิผล รวมถึงจะต้องจัดให้มีกลไกในการพิจารณาถึงประเภทของเหตุการณ์ ปริมาณ และต้นทุนที่เกิดขึ้น สุดท้ายจะต้องมีการรวบรวม จัดเก็บ และดูแลรักษา หลักฐานต่าง ๆ ที่เกี่ยวกับการดำเนินการจากเหตุการณ์ต่าง ๆ ที่เกิดขึ้น เพื่อใช้เป็นประโยชน์ในการดำเนินการทางคดีความ ถ้าจำเป็น

2.2.12.10 การบริหารความต่อเนื่องในการดำเนินธุรกิจ

ในข้อกำหนดนี้ จะระบุให้องค์กรต้องมีการจัดทำกระบวนการในการสร้างความต่อเนื่องทางธุรกิจ (Business Continuity) ทั่วทั้งองค์กร ทั้งนี้จะต้องนำข้อกำหนดความมั่นคงปลอดภัยมารวมไว้ในการบริหารความต่อเนื่องทางุธุรกิจด้วย โดยจะต้องมีการระบุถึงเหตุการณ์ ทีจะมีผลให้เกิดการหยุดชะงักของกระบวนการธุรกิจ รวมถึงโอกาสที่จะเกิดขึ้น และผลกระทบที่ตามมาถ้าเหตุการณ์นั้นได้เกิดขึ้นจริง

จากนั้นให้ทำการพัฒนาแผนความต่อเนื่องทางธุรกิจ ซึ่งรวมประเด็นด้านความมั่นคงปลอดภัยของสารสนเทศไว้ด้วย และมีการนำไปปฏิบัติ เพื่อให้มั่นใจได้ถึงความพร้อมของสารสนเทศในระดับที่ยอมรับได้ ในกรณีที่เกิดเหตุการณ์ที่ทำให้ธุรกิจเกิดการหยุดชะงัก หรือความผิดพลาดขึ้น

เมื่อมีการจัดทำแผนความต่อเนื่องทางธุรกิจแล้ว จะต้องจัดให้มีการทดสอบ และปรับปรุงแผนความต่อเนื่องในการดำเนินธุรกิจอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ถึงความทันสมัย และความมีประสิทธิผล

2.2.12.11 ความสอดคล้องตามข้อกำหนด

ในหัวข้อหลักของการควบคุมนี้ ได้แบ่งออกเป็น 3 ส่วนประกอบด้วย การดำเนินการให้สอดคล้องตามข้อกำหนดทางกฎหมาย (Legal Requirements) การดำเนินการให้สอดคล้องตามนโยบายความมั่นคงปลอดภัย มาตรฐาน และข้อกำหนดทางเทคนิค และการดำเนินการตรวจประเมินระบบสารสนเทศ (Information System Audit)

ในการดำเนินการตามข้อกำหนดทางกฎหมาย จะเริ่มต้นจากการระบุถึงข้อกำหนดทางกฎหมายต่าง ๆ รวมถึงระเบียบ ข้อบังคับ ประกาศ และข้อกำหนดในสัญญาต่าง ๆ ที่เกี่ยวข้อง โดยจะต้องมีการจัดทำเป็นเอกสาร และมีการปรับปรุงให้ทันสมัยอยู่เสมอ รวมถึงมีการกำหนดแนวทางในการดำเนินการขององค์กรเพื่อให้สอดคล้องตามข้อกำหนดต่าง ๆ ด้วย

นอกจากนั้นยังต้องกำหนดให้มีแนวทางในการดำเนินงาน เพื่อปกป้องจากการดำเนินงานในลักษณะที่เป็นการละเมิดสิทธิหรือทรัพย์สินทางปัญญา (Intellectual Property Rights, IPR) เช่น การใช้ผลิตภัณฑ์ซอฟต์แวร์ที่ไม่ถูกต้อง รวมถึงจะต้องมีการดำเนินการในการดูแลป้องกันข้อมูลที่สำคัญขององค์กร และข้อมูลส่วนบุคคล จากการสูญหาย เสียหาย หรือมีการปลอมแปลง ให้สอดคล้องกับข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ ข้อกำหนดในสัญญา และข้อกำหนดทางธุรกิจ

นอกจากนั้น จะต้องกำหนดให้มีมาตรการในการป้องกันการนำอุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศ ไปใช้ผิดวัตถุประสงค์ และมีการกำหนดมาตรการในการควบคุมการเข้ารหัสข้อมูลให้สอดคล้องตามข้อตกลง ข้อกฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้องด้วย

ในส่วนของการดำเนินการตามนโยบาย และมาตรฐาน จะเป็นหน้าที่ของผู้บังคับบัญชาในหน่วยงานต่าง ๆ ในการดูแลให้มั่นใจว่าพนักงานในการดูแล ได้ปฏิบัติงานอย่างถูกต้อง ตามนโยบายและมาตรฐานความมั่นคงปลอดภัย รวมถึงจะต้องมีการตรวจสอบระบบสารสนเทศ เพื่อยืนยันความสอดคล้องตามข้อกำหนดต่าง ๆ อย่างต่อเนื่องด้วย

ในการตรวจประเมินระบบสารสนเทศ (Information System Audit) จะต้องมีการวางแผนข้อกำหนดการตรวจประเมิน รวมถึงการตรวจสอบระบบการปฏิบัติงานอย่างระมัดระวัง และดำเนินการโดยให้เกิดผลกระทบต่อการหยุดชะงักของกระบวนการทางธุรกิจน้อยที่สุด รวมถึงจะต้องมีการกำหนดมาตรการในการเข้าถึงเครื่องมือที่ใช้ในการตรวจประเมินระบบสารสนเทศ เพื่อป้องกันการนำไปใช้งานผิดวัตถุประสงค์

2.3 การประเมินการปฏิบัติการเกี่ยวกับช่องโหว่และสินทรัพย์ ภัยคุกคามที่สำคัญยิ่งยวด (Operationally Critical Threat, Asset and Vulnerability Evaluation: OCTAVE)

การรักษาความมั่นคงปลอดภัยเป็นกฎระเบียบที่ซับซ้อน ทั้งในองค์ประกอบด้านองค์กรและเทคโนโลยี หากพิจารณาตามบทบาทขององค์กร องค์กรด้านการเงินต้องมีการปกป้องข้อมูลส่วนตัวของลูกค้า นโยบายด้านความมั่นคงปลอดภัยของบริษัทต้องมีข้อกำหนดในการเข้าถึงข้อมูลตามหน้าที่อย่างชัดเจน การจัดการด้านความมั่นคงปลอดภัยเป็นการลงทุนที่สูงเพื่อให้มั่นใจว่าองค์กรได้ดำเนินตามนโยบายการรักษาความมั่นคงปลอดภัย ตัวอย่างเช่น ระบบหลักทั้งหมดมีกลไกการควบคุมการจำกัดการเข้าถึงทรัพยากรของระบบ เมื่อพนักงานเริ่มทำงานในบริษัทก็จะได้รับสิทธิในการเข้าใช้ทรัพยากรของระบบตามบทบาทหน้าที่ของแต่ละคน โดยปฏิบัติตามนโยบายควบคุมการเข้าถึงที่บังคับโดยกลไกทางเทคโนโลยี

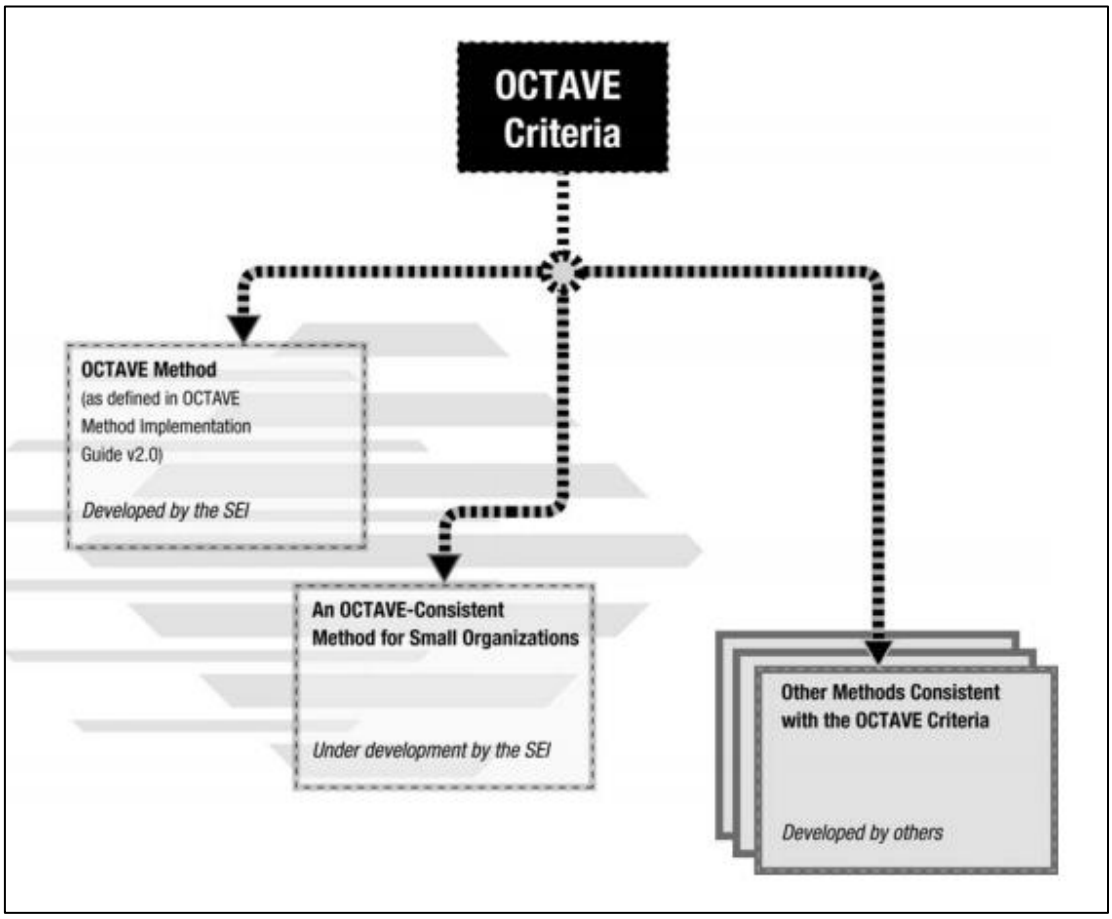
อย่างไรก็ตามเมื่อพนักงานออกจากบริษัทไปแล้ว สิทธิ์การเข้าถึงระบบของพวกเค้ามักจะไม่ได้ถูกยกเลิก แม้พนักงานเหล่านั้นจะไม่ได้ทำงานให้องค์กรแล้ว แต่พวกเค้าก็ยังสามารถเข้าถึงระบบและข้อมูลทางการเงินได้ นอกจากนั้น เมื่อพนักงานเปลี่ยนหน้าที่ความรับผิดชอบภายในบริษัท พวกเค้าไม่เพียงแต่จะได้รับสิทธิ์การเข้าถึงตามหน้าที่ใหม่เท่านั้น พวกเค้ายังคงมีสิทธิ์การเข้าถึงตามหน้าที่เก่าอีกด้วย แม้ว่าขั้นตอนเหล่านนี้มีไว้เพื่อให้สิทธิ์การเข้าถึงที่เหมาะสมแก่

พนักงานเมื่อเปลี่ยนระดับชั้นตำแหน่ง แต่ขั้นตอนเหล่านั้นไม่ได้ยกเลิกสิทธิ์การเข้าถึงที่ไม่จำเป็น พนักงานที่ทำงานในองค์กรมาหลายปี มีสิทธิ์การเข้าถึงแทบทุกระบบที่ต้องการ แม้ว่าองค์กรจะมีเทคโนโลยีที่บังคับใช้สำหรับบทบาทการเข้าถึงข้อมูลและระบบ แต่ด้วยการปฏิบัติจริงในองค์กรขั้นตอนเหล่านี้ก็ยังมีข้อบกพร่อง

ระบบสารสนเทศเป็นสิ่งที่จำเป็นสำหรับองค์กร เนื่องจากแทบทุกข้อมูลถูกจัดเก็บและเข้าถึงในรูปแบบดิจิทัล เราพึ่งพาข้อมูลดิจิทัล ที่สามารถเข้าถึงได้ เชื่อถือได้ และได้รับการป้องกันจากการนำไปใช้ในทางที่ผิด ระบบต่าง ๆ เชื่อมต่อกันในรูปแบบที่เราไม่สามารถจินตนาการได้จากเมื่อ 10 ปีก่อน ระบบเครือข่ายทำให้เราสามารถเข้าถึงข้อมูลได้อย่างที่ไม่เคยมีมาก่อน แต่โชคไม่ดีที่มันก็เป็นการเปิดเผยข้อมูลต่อภัยคุกคามใหม่ ๆ ด้วย องค์กรควรมีกระบวนการให้พนักงานเข้าใจถึงความเสี่ยงและสร้างกลยุทธ์เพื่อจัดการความเสี่ยงนั้นด้วย

การประเมินการปฏิบัติการเกี่ยวกับช่องโหว่และสินทรัพย์ ภัยคุกคามที่สำคัญยิ่งยวด (Operationally Critical Threat, Asset and Vulnerability Evaluation[sm]: OCTAVE[sm]) ช่วยให้บุคลากรขององค์กรสามารถจัดประเภทเครือข่ายที่ซับซ้อนขององค์กรและประเด็นทางเทคโนโลยีและกำหนดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ OCTAVE กำหนดวิธีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูลที่ครอบคลุม เป็นระบบ ตรงตามบริบทและทิศทางของตนเอง กระบวนการต้องการทีมวิเคราะห์แบบสหวิทยาการทางธุรกิจและบุคลากรด้านเทคโนโลยีสารสนเทศขององค์กรเพื่อเป็นผู้นำในกระบวนการประเมิน

องค์ประกอบ หรือข้อกำหนด ของวิธีการ OCTAVE มีอยู่ในชุดของเกณฑ์ มีหลายวิธีที่สอดคล้องกับเกณฑ์ แต่เกณฑ์ OCTAVE จะมีเพียงแค่หนึ่งชุดเท่านั้น ณ จุดนี้ เราได้พัฒนาวิธีการหนึ่งที่สอดคล้องกับเกณฑ์ ซึ่งเป็นวิธีการที่เราได้ทำเป็นเอกสารชื่อ OCTAVE Method Implementation Guide, v2.0 ซึ่งออกแบบโดยคำนึงถึงองค์กรขนาดใหญ่ ในปัจจุบันได้พัฒนาวิธีการสำหรับองค์กรขนาดเล็กแล้วด้วย นอกจานั้น องค์กรแบบอื่นยังสามารถกำหนดวิธีการเฉพาะแบบขององค์กรที่สอดคล้องกับเกณฑ์ได้ด้วย ภาพประกอบที่ 2.3 แสดงให้เห็นถึงจุดนี้



ภาพประกอบที่ 2.3 เกณฑ์ OCTAVE

2.3.1 ภูมิหลัง

กรอบการประเมินการปฏิบัติการเกี่ยวกับช่องโหว่และสินทรัพย์ ภัยคุกคามที่สำคัญยิ่งยวด (Operational Critical Threat, Asset and Vulnerability Assessment) (OCTAVE Framework กรอบนี้เป็นรายละเอียดสำหรับการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเป้าหมายในองค์กรขนาดใหญ่ รายงานด้านเทคนิคแสดงให้เห็นถึงไดอะแกรมการไหลของสารสนเทศ (Data Flow Diagram) ที่มีรายละเอียดองค์ประกอบของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ: ชุดของกระบวนการ 8 ขั้นตอน ซึ่งในแต่ละขั้นตอนต้องการ ตัวป้อน (Inputs), กิจกรรม (Activities) และผลลัพธ์ (Outputs)

เมื่อเราเริ่มพัฒนากรอบ เป้าหมายของเราคือกำหนดความต้องการของวิธีการทั่วไปสำหรับการประเมินและการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล อย่างไรก็ตามเราพบว่าการจัดทำวิธีการทั่วไปในองค์กรขนาดเล็กที่มีพนักงาน 10 คนจะดูแตกต่างจากบริษัทข้ามชาติขนาด

ใหญ่ ดังนั้นเราจึงเชื่อว่าเราจำเป็นตรวจสอบองค์กรทั้ง 2 แบบก่อนจึงกำหนดความต้องการสำหรับวิธีการประเมินทั่วไปได้

เราได้ออกแบบกระบวนการ OCATVE สำหรับใช้กับองค์กรขนาดใหญ่ และต่อมาเราได้พัฒนากระบวนการให้ใช้กับองค์กรขนาดเล็กได้ด้วย การพัฒนาและทดสอบวิธีการเหล่านี้ ช่วยให้เรากำหนดความต้องการที่ทั่วไป (หรือสำคัญ) ข้อกำหนดของวิธีการ OCTAVE และนำไปสู่การปรับกรอบไปสู่เกณฑ์ OCTAVE โดยมีวัตถุประสงค์ดังข้อ 2.3.2

2.3.2 วัตถุประสงค์

ในเอกสารรายงานทางเทคนิคของเกณฑ์ OCTAVE ฉบับนี้ มีเป้าหมายในการเขียนคือกำหนดวิธีการทั่วไปสำหรับการประเมินและการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เอกสารฉบับนี้ไม่ได้ให้รายละเอียดการจัดทำที่เฉพาะเจาะจงเกี่ยวกับวิธีดำเนินการ เราส่งเสริมให้องค์กรพัฒนาวิธีการให้สอดคล้องกับเกณฑ์ OCTAVE ดังรายละเอียดในข้อ 2.3.3

2.3.3 OCTAVE คืออะไร?

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศจะต้องยึดประเด็นทั้งในส่วนองค์กรและส่วนเทคโนโลยีเพื่อให้มีประสิทธิภาพ ต้องระบุการประมวลผลโครงสร้างพื้นฐานที่พนักงานใช้เป็นส่วนหนึ่งในการทำงานของพวกเขา ดังนั้นการประเมินผลต้องรวมบริบทของพนักงานแต่ละคนที่ใช้โครงสร้างพื้นฐานเข้ากับวัตถุประสงค์ในการดำเนินธุรกิจขององค์กร เช่นเดียวกับประเด็นด้านความมั่นคงปลอดภัยทางเทคโนโลยีที่เกี่ยวข้องกับโครงสร้างพื้นฐาน โดยแนวคิดสำคัญของเกณฑ์ OCTAVE แสดงในข้อ 2.3.4

2.3.4 แนวคิดสำคัญของเกณฑ์ OCTAVE

เราใช้การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อปรับปรุงการรักษาความมั่นคงปลอดภัยขององค์กร ตั้งแต่ที่องค์กรส่วนมากก้าวเข้าสู่การใช้ข้อมูลอิเล็กทรอนิกส์ในการดำเนินธุรกิจ ต้องมีการปกป้องไม่ให้ใช้ข้อมูลในทางที่ผิด ความสามารถขององค์กรที่จะทำภารกิจให้สำเร็จตามวัตถุประสงค์ขององค์กรนั้นเกี่ยวข้องโดยตรงกับการประมวลผลโครงสร้างพื้นฐานและลักษณะการใช้งานของพนักงานที่มีต่อโครงสร้างพื้นฐาน สำหรับองค์กรที่จะประสบความสำเร็จ พนักงานในองค์กรจะต้องเข้าใจว่าข้อมูลที่เกี่ยวกับสินทรัพย์อันไหนที่สำคัญและต้องได้รับการปกป้อง นั่นหมายถึงพนักงานในองค์กรจำเป็นต้องมีส่วนร่วมในการประเมิน

OCTAVE คือการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศด้วยตัวเอง แนวคิดหลักของ OCTAVE คือสถานการณ์ที่พนักงานขององค์กรบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเทศด้วยตนเองสำหรับองค์กร พนักงานขององค์กรประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศด้วยตนเอง และรับผิดชอบในการตัดสินใจเกี่ยวกับการปรับปรุงความมั่นคงปลอดภัยสารสนเทศขององค์กร ใน OCTAVE ทีมสหวิทยาการ ที่เรียกว่า ทีมวิเคราะห์ เป็นผู้นำในการประเมิน

ทีมวิเคราะห์ประกอบด้วยพนักงานจากหน่วยงานทางธุรกิจและหน่วยงานทาง IT เนื่องจากความมั่นคงปลอดภัยสารสนเทศรวมไปถึงประเด็นทางธุรกิจและทางเทคโนโลยี พนักงานจากหน่วยงานทางธุรกิจ เข้าใจว่าข้อมูลที่สำคัญ ที่จะทำให้งานของเขาสำเร็จ และทราบถึงวิธีการเข้าถึงและใช้ข้อมูลนั้น พนักงานด้าน IT เข้าใจประเด็นเกี่ยวกับวิธีการกำหนดค่าการประมวลผล โครงสร้างพื้นฐาน และสิ่งใดที่สำคัญต่อการทำงานของโครงสร้างพื้นฐาน ทั้ง 2 มุมมองมีความสำคัญในการทำความเข้าใจความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร

ความเสี่ยงคือความเป็นไปได้ที่จะเกิดความเสียหายหรือสูญเสีย สามารถแบ่งออกเป็น 3 องค์ประกอบพื้นฐาน: สินทรัพย์, ภัยคุกคาม, และช่องโหว่ ดังนั้น การประเมินความเสี่ยงด้านความมั่นคงสารสนเทศ ต้องคำนึงถึงความเสี่ยงของทั้ง 3 องค์ประกอบด้วย OCTAVE เป็นวิธีการประเมินความเสี่ยง ที่กำหนดให้ทีมวิเคราะห์ดำเนินการ:

(1) ระบุข้อมูลสินทรัพย์ที่เกี่ยวข้อง (เช่น สารสนเทศและระบบ) ที่สำคัญต่อองค์กร

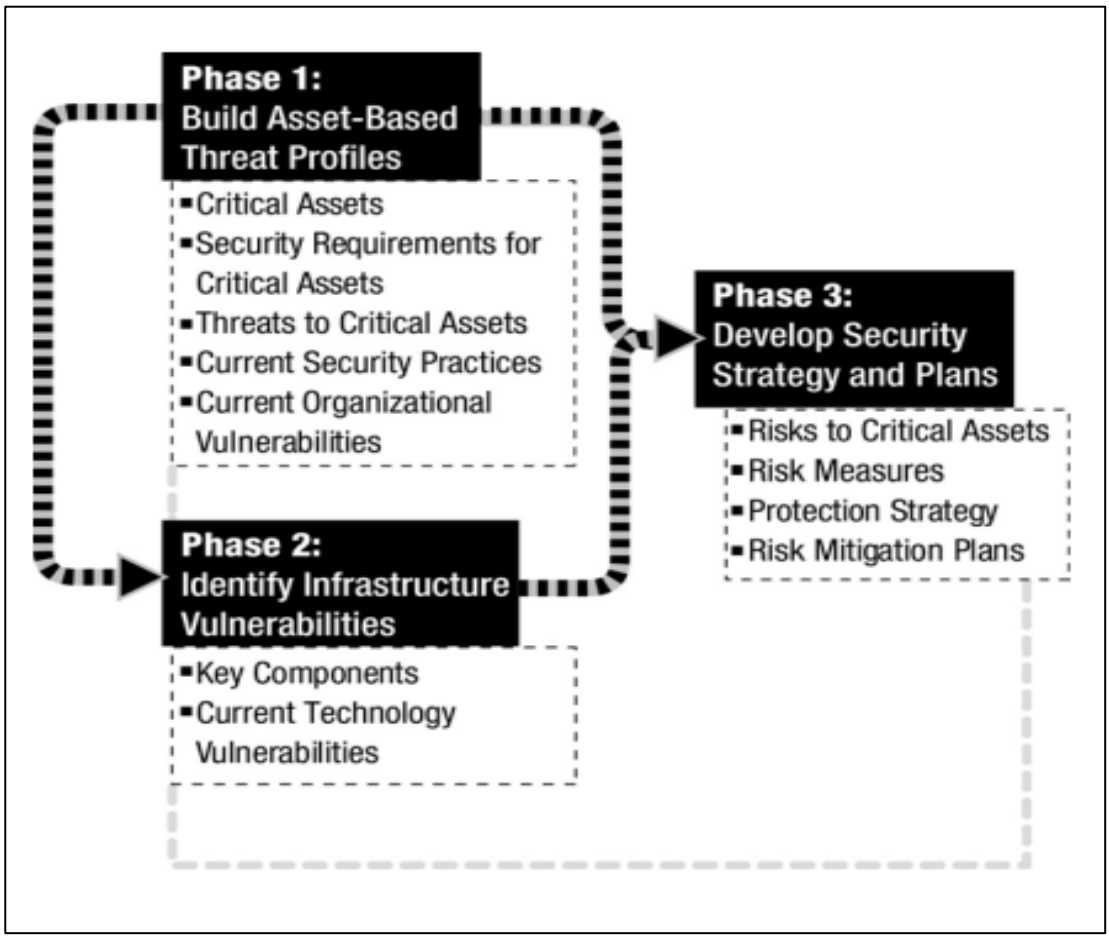
(2) มุ่งเน้นกิจกรรมการวิเคราะห์ความเสี่ยงเพื่อประเมินค่าของสินทรัพย์เหล่านั้นว่าสินทรัพย์ใดมีความสำคัญที่สุดแก่องค์กร

OCTAVE ต้องการให้ทีมวิเคราะห์พิจารณาความสัมพันธ์ระหว่างสินทรัพย์ที่สำคัญ ภัยคุกคามที่มีต่อสินทรัพย์เหล่านั้น และช่องโหว่ (ทั้งด้านองค์กรและด้านเทคนิค) ทำให้ทราบถึงภัยคุกคามที่มีต่อสินทรัพย์ เพื่อให้ทีมวิเคราะห์ประเมินความเสี่ยงในบริบทการดำเนินงาน

เมื่อทีมดำเนินการ OCTAVE เรียบร้อยแล้ว จะสร้างกลยุทธ์การปกป้องสำหรับการปรับปรุงองค์กรและแผนบรรเทาความเสี่ยง เพื่อลดความเสี่ยงให้กับสินทรัย์ที่สำคัญขององค์กร ดังนั้น OCTAVE จึงรวมทั้งในด้านกลยุทธ์และมุมมองยุทธวิธีด้านความเสี่ยง ซึ่งรายละเอียดขั้นตอนการดำเนินงานจะแสดงในข้อ 2.3.5

2.3.5 ขั้นตอนสำหรับการดำเนินการ OCTAVE (สามด้าน-สามขั้นตอน)

ด้านองค์กร ด้านเทคโนโลยี และด้านการวิเคราะห์ ของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ นำไปสู่กวิธีการ 3 ขั้นตอน OCTAVE จัดขึ้นโดยมีพื้นฐานอยู่บน 3 ด้านนี้ (ดังที่แสดงให้เห็นในภาพประกอบที่ 2.4) ช่วยให้พนักงานขององค์กรสามารถรวมบรวมภาพที่ซับซ้อนของความต้องการในการรักษาความมั่นคงปลอดภัยขององค์กร



ภาพประกอบที่ 2.4 ขั้นตอน OCTAVE

2.3.5.1 ขั้นที่ 1 สร้างโพร์ไฟล์ภัยคุกคามสินทรัพย์ คือการประเมินองค์กร พนักงานขององค์กรให้ความคิดเห็นว่าสิ่งใดสำคัญแก่องค์กร (ข้อมูลที่เกี่ยวกับสินทรัพย์) และสิ่งที่กำลังทำอยู่เพื่อปกป้องสินทรัพย์เหล่านั้น ทีมวิเคราะห์พิจารณาข้อมูลและเลือกว่าสินทรัพย์ใดที่สำคัญต่อองค์กร ทีมจะอธิบายถึงสิ่งที่ต้องการในการรักษาความมั่นคงปลอดภัย สำหรับสินทรัพย์ที่สำคัญและระบุภัยคุกคามที่มีต่อสินทรัพย์ที่สำคัญ สร้างโพร์ไฟล์ภัยคุกคาม

2.3.5.2 ขั้นที่ 2 ระบุช่องโหว่ของโครงสร้างพื้นฐาน คือการประเมินข้อมูลโครงสร้างพื้นฐาน ทีมวิเคราะห์จะระบุคีย์ของระบบข้อมูลสารสนเทศและองค์ประกอบที่เกี่ยวข้องกับสินทรัพย์ที่สำคัญ ทีมจะตรวจสอบคีย์องค์ประกอบสำหรับจุดอ่อน (ช่องโหว่ทางเทคโนโลยี) ที่นำไปสู่การกระทำที่ไม่ได้รับอนุญาตต่อสินทรัพย์ที่สำคัญ

2.3.5.3 ขั้นตอนที่ 3 พัฒนากลยุทธ์การรักษาความมั่นคงปลอดภัยและการวางแผน คือระหว่างการประเมินในขั้นตอนนี้ ทีมวิเคราะห์จะระบุความเสี่ยงที่มีต่อสินทรัพย์ที่สำคัญขององค์กรและตัดสินใจว่าจะดำเนินการเช่นไร ทีมสร้างกลยุทธ์การปกป้องสำหรับองค์กรและแผนบรรเทาความเสี่ยงสำหรับสินทรัพย์ที่สำคัญ โดยมีพื้นฐานจากการวิเคราะห์ข้อมูลที่รวบรวมได้ กิจกรรมสำหรับการดำเนินการ OCTAVE ต่อไปจะแสดงในข้อ 2.3.6

2.3.6 ส่วนของความต่อเนื่อง

OCTAVE ช่วยให้มองเห็นภาพรวมขององค์กรในความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่มีอยู่ในปัจจุบัน ในการดำเนินงาน OCTAVE ทีมวิเคราะห์จะดำเนินกิจกรรม ดังนี้:

(1.) ระบุความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

(2.) วิเคราะห์ความเสี่ยงเพื่อจัดลำดับความสำคัญ

(3.) วางแผนเพื่อปรับปรุงโดยพัฒนากลยุทธ์การป้องกันสำหรับการปรับปรุงองค์กรและแผนการบรรเทาความเสี่ยงเพื่อลดความเสี่ยงต่อสินทรัพย์ที่สำคัญขององค์กร

องค์กรจะไม่ดำเนินการปรับปรุงจนกว่าจะจัดทำตามแผน กิจกรรมการปรับปรุงเหล่านี้จะดำเนินการหลัง OCTAVE เสร็จสิ้น หลังจาก OCTAVE ทีมวิเคราะห์ หรือพนักงานที่ได้กำหนดไว้ดำเนินการดังนี้

(1.) วางแผนจัดทำกลยุทธ์การปกป้องและแผนการบรรเทาความเสี่ยง โดยพัฒนารายละเอียดแผนปฏิบัติการ รายละเอียดกิจกรรมรวมไปถึงการวิเคราะห์ต้นทุน ระหว่างกลยุทธ์และการปฏิบัติการ และผลลัพธ์ในรายละเอียดการจัดทำแผน

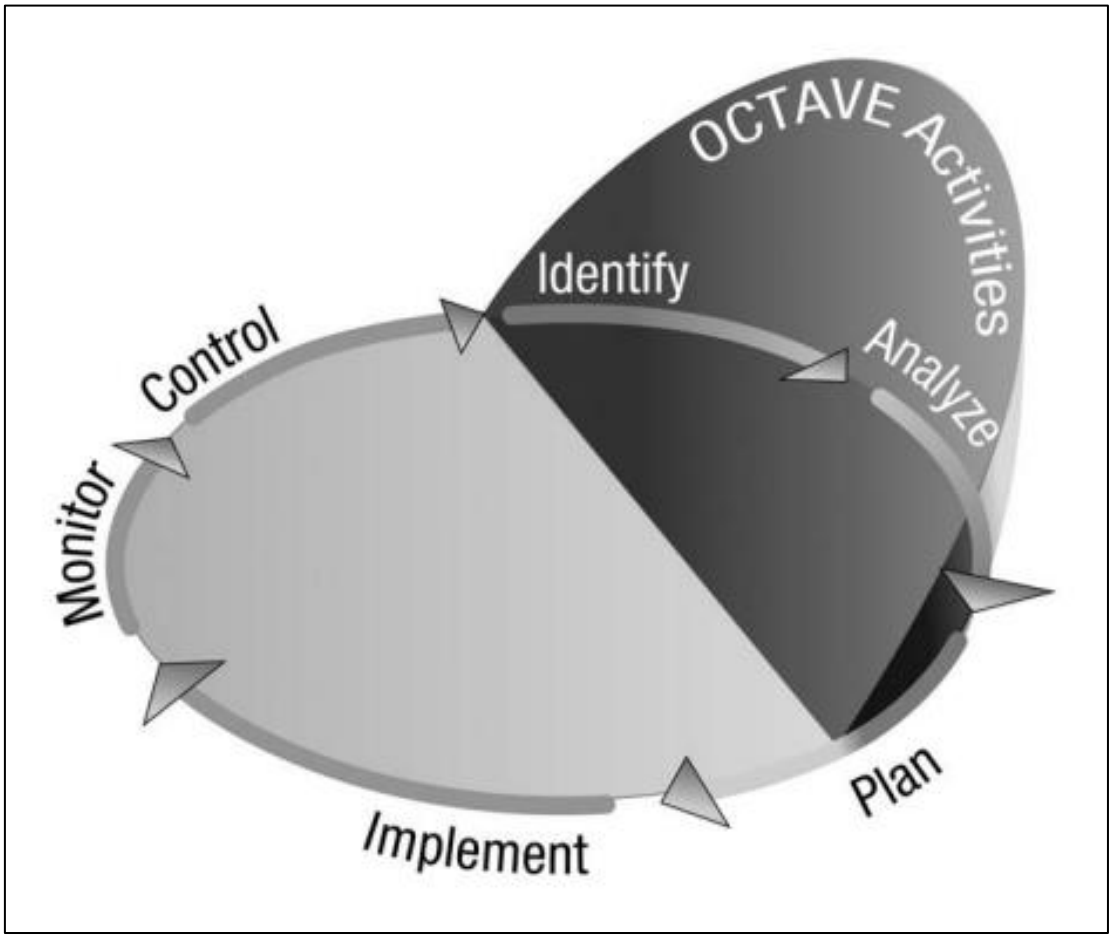
(2.) จัดทำรายละเอียดแผนปฏิบัติการ

(3.) ตรวจสอบแผนปฏิบัติการสำหรับกำหนดการเพื่อให้เกิดประสิทธิภาพที่แท้จริง กิจกรรมรวมไปถึงการเฝ้าระวังด้านความเสี่ยงสำหรับการเปลี่ยนแปลงต่าง ๆ

(4.) ควบคุมรูปแบบต่าง ๆ ในแผนดำเนินการโดยการแก้ไขให้เหมาะสม

โน้ต: กิจกรรมเหล่านี้ไม่มีอะไรมากไปกว่าวัฏจักร PDCA

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เป็นส่วนหนึ่งในกิจกรรม การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร OCTAVE คือกิจกรรมการประเมิน ไม่ใช่กระบวนการที่ต่อเนื่อง ดังนั้นจึงมีการกำหนดจุดเริ่มต้นและจุดจบ ภาพประกอบที่ 2.5 แสดงความสัมพันธ์ระหว่างกิจกรรมเหล่านี้ และจุดที่เหมาะสมกับ OCTAVE นอกจากนี้ ควรจะทราบว่ามีกิจกรรมการระบุและวิเคราะห์อย่างต่อเนื่อง



ภาพประกอบที่ 2.5 OCTAVE และกิจกรรมบริหารความเสี่ยง

องค์กรจำเป็นต้อง “รีเซ็ต” พื้นฐานของ OCTAVE โดยดำเนินการ OCTAVE อีกครั้ง ช่วงเวลาในการประเมินสามารถกำหนดไว้ล่วงหน้าได้ (เช่น กำหนดไว้เป็นรายปี) หรือสำหรับใช้งานตามเหตุการณ์ที่สำคัญ (เช่น การปรับโครงสร้างองค์กร หรือออกแบบโครงสร้างพื้นฐานขององค์กรใหม่) ในระหว่างการประเมิน องค์กรสามารถระบุความเสี่ยงใหม่ ๆ ได้เป็นระยะ วิเคราะห์ความเสี่ยงใหม่ที่มีความสัมพันธ์กับความเสี่ยงที่มีอยู่ และพัฒนาแผนบรรเทาความเสี่ยงเหล่านั้น

2.3.7 โครงสร้างของเกณฑ์ OCTAVE

เกณฑ์ OCTAVE คือชุดของหลักการ, คุณลักษณะ และผลลัพธ์ หลักการคือแนวคิดพื้นฐานที่ขับเคลื่อนธรรมชาติของการประเมิน กำหนดปรัชญาที่รูปแบบของกระบวนการประเมิน ตัวอย่างเช่น กำหนดทิศทางของตนเองเป็นส่วนหนึ่งของหลักการ OCTAVE แนวคิดของการกำหนดทิศทางของตนเองหมายความว่าพนักงานขององค์กรอยู่ในตำแหน่งที่เหมาะสมสำหรับการประเมินและตัดสินใจ

ข้อกำหนดของการประเมินจะเป็นปรากฏในคุณลักษณะและผลลัพธ์ คุณลักษณะคือลักษณะที่โดดเด่น หรือลักษณะเฉพาะของการประเมิน คือข้อกำหนดองค์ประกอบพื้นฐานของวิธีการ OCTAVE และกำหนดสิ่งที่สำคัญเพื่อทำให้การประเมินผลสำเร็จทั้งในด้านกระบวนการและมุมมองขององค์กร คุณลักษณะที่ได้มาจากหลักการ OCTAVE ตัวอย่างเช่น หนึ่งในคุณลักษณะของ OCTAVE คือทีมสหวิทยาการ (ทีมวิเคราะห์) เป็นพนักงานขององค์กรที่เป็นผู้นำในการประเมิน หลักการของการสร้างทีมวิเคราะห์คือการกำหนดทิศทางของตนเอง

ท้ายที่สุด สิ่งที่ได้คือผลลัพธ์ที่ต้องการของการประเมินในแต่ละขั้นตอน มีการกำหนดผลลัพธ์ที่ทีมวิเคราะห์จะต้องทำให้สำเร็จในแต่ละขั้นตอน

2.3.8 หลักการของ OCTAVE

หลักการเป็นแนวคิดพื้นฐานที่กำหนดปรัชญาของกระบวนการประเมิน หลักการกำหนดรูปแบบและเป็นพื้นฐานของการประเมิน เราได้จัดกลุ่มหลักการไว้เป็น 3 กลุ่ม ดังต่อไปนี้

(1.) หลักการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ: เป็นประเด็นสำคัญเป็นรากฐานของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศอย่างมีประสิทธิภาพ มีดังนี้

(1.1) ทิศทางของตนเอง

(1.2) มาตรการที่ปรับเปลี่ยนได้

(1.3) กระบวนการที่กำหนด

(1.4) พื้นฐานของกระบวนการที่ต่อเนื่อง

(2.) หลักการบริหารความเสี่ยง: เป็นหลักการพื้นฐานทั่วไป เพื่อดำเนินการบริหารความเสี่ยงให้เป็นไปอย่างมีประสิทธิภาพ มีดังนี้

(2.1) มองถึงอนาคต

(2.2) ให้ความสำคัญกับเรื่องสำคัญ

(2.3) การจัดการแบบบูรณาการ

(3.) หลักการองค์กรและวัฒนธรรม: คือลักษณะขององค์กรในด้านวัฒนธรรมที่สำคัญในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

(3.1) การสื่อสารแบบเปิด

(3.2) มุมมองที่กว้างไกล

(3.3) การทำงานเป็นทีม

หลักการดังกล่าวแสดงในภาพประกอบที่ 2.6

ภาพประกอบที่ 2.6 หลักการของ OCTAVE

2.3.9 หลักการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

ในส่วนนี้ มุ่งเน้นที่หลักการที่เป็นพื้นฐานของการประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศอย่างมีประสิทธิภาพ โดยเริ่มที่กำหนดทิศทางของตนเอง

2.3.9.1 ทิศทางของตนเอง

ทิศทางของตนเอง อธิบายถึงสถานการณ์ที่พนักงานในองค์กรจัดการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรด้วยตนเอง พนักงานเหล่านี้รับผิดชอบโดยตรงในกิจกรรมบริหารความเสี่ยงและตัดสินใจเกี่ยวกับความมั่นคงปลอดภัยขององค์กร การกำหนดทิศทางของตนเองกำหนดไว้ดังนี้

(1) รับผิดชอบด้านความมั่นคงปลอดภัยของข้อมูลโดยต้องเป็นผู้นำในการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และในกระบวนการบริหารความเสี่ยง

(2) การตัดสินใจขั้นสุดท้ายเกี่ยวกับความมั่นคงปลอดภัยขององค์กร รวมไปถึงการปรับปรุงและการดำเนินการ

2.3.9.2 มาตรการที่ปรับเปลี่ยนได้

กระบวนการประเมินที่ยืดหยุ่นสามารถปรับเปลี่ยนตามเทคโนโลยีที่เปลี่ยนแปลงและก้าวหน้า ไม่ได้กำหนดเป็นรูปแบบที่ตายตัวสำหรับภัยคุกคามหรือแนวปฏิบัติในปัจจุบันที่ยอมรับว่า “ดีที่สุด” เนื่องจากความมั่นคงปลอดภัยสารสนเทศหรือเทคโนโลยีสารสนเทศมีการเปลี่ยนแปลงที่รวดเร็ว ดังนั้นจึงเป็นเรื่องสำคัญที่กระบวนการประเมินองค์กรจึงต้องปรับเปลี่ยนตามด้วย มาตรการที่ปรับเปลี่ยนได้กำหนดไว้ดังนี้

(1) แค็ตตาล็อกของสารสนเทศในปัจจุบันเป็นตัวกำหนดการดำเนินการด้านความมั่นคงปลอดภัย ทราบถึงภัยคุกคาม และรู้ถึงจุดอ่อนด้านเทคโนโลยี (ช่องโหว่)

(2) กระบวนการประเมินเอื้อต่อการเปลี่ยนแปลงของแค็ตตาล็อกของสารสนเทศ

2.3.9.3 กระบวนการที่กำหนด

กระบวนการที่กำหนดอธิบายถึงความจำเป็นสำหรับโปรแกรมการประเมินความมั่นคงปลอดภัยสารสนเทศ โดยอาศัยขั้นตอนการประเมินผลที่กำหนดและได้มาตรฐาน การกำหนดกระบวนการประเมินสามาถช่วยจัดระเบียบกระบวนการ สร้างความมั่นใจในแต่ละระดับของการประเมินมีความเหมาะสม กระบวนการที่กำหนด กำหนดไว้ดังนี้

(1) มอบหมายหน้าที่ความมับผิดชอบในการดำเนินการประเมิน

(2) กำหนดกิจกรรมการประเมินทั้งหมด

(3) กำหนดการใช้งานเครื่องมือทั้งหมด เอกสารงาน และแค็ตตาล็อกสารสนเทศ ที่ต้องใช้ในการประเมิน

(4) สร้างรูปแบบสำหรับการจัดทำเอกสารด้านผลการประเมิน

2.3.9.3 พื้นฐานของกระบวนการที่ต่อเนื่อง

องค์กรต้องจัดทำแนวปฏิบัติตามกลยุทธ์การรักษาความมั่นคงปลอดภัยและวางแผนเพื่อการปรับปรุงการรักษาความมั่นคงปลอดภัย โดยดำเนินแก้ไขแนวปฏิบัติเหล่านี้ องค์กรสามารถเริ่มต้นได้ด้วยการกำหนดแนวปฏิบัติด้านความมั่นคงปลอดภัยที่ดี ทำให้เป็นส่วนหนึ่งในการดำเนินงานขององค์กร การปรับปรุงการรักษาความมั่นคงปลอดภัยคือกระบวนการที่ต่อเนื่อง และผลลัพธ์ของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสร้างรากฐานสำหรับกระบวนการปรับปรุงที่ต่อเนื่อง รากฐานสำหรับกระบวนการที่ต่อเนื่องกำหนดไว้ดังนี้

(1.) กำหนดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศโดยใช้กระบวนการประเมินผลที่กำหนด

(2.) ดำเนินการตามผลลัพธ์ที่ได้จากการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

(3.) กำหนดสมรรถนะในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศในแต่ละช่วงเวลา

(4.) จัดทำกลยุทธ์การรักษาความมั่นคงปลอดภัยและวางแผนที่รวมวิธีปฏิบัติที่ดีเข้าไว้ด้วยกันสำหรับปรับปรุงการรักษาความมั่นคงปลอดภัย

2.3.10 หลักการบริหารความเสี่ยง

เป็นหลักการที่กว้างขึ้น โดยมุ่งเน้นที่แนวคิดทั่วไปเพื่อให้วิธีการบริหารความเสี่ยงมีประสิทธิภาพ

2.3.10.1 มองไปข้างหน้า

การมองไปข้างหน้าจำเป็นต้องมีบุคลากรขององค์กรที่มองการณ์ไกลกว่าปัญหาในปัจจุบัน โดยมุ่งเน้นไปที่ความเสี่ยงของสินทรัพย์ที่สำคัญที่สุดขององค์กร มุ่งเน้นไปที่การจัดการความไม่แน่นอน โดยตรวจสอบความสัมพันธ์ระหว่างสินทรัพย์ ภัยคุกคาม และช่องโหว่ และตรวจสอบผลลัพธ์ที่ส่งผลต่อวัตถุประสงค์และภารกิจขององค์กร การมองไปข้างหน้ากำหนดไว้ดังนี้

(1.) คิดเกี่ยวกับวันพรุ่งนี้ มุ่มเน้นที่การจัดการความไม่แน่นอนโดยแยกเป็นประเภทของความเสี่ยง

(2.) การจัดการทรัพยากรขององค์กรและกิจกรรม จากความไม่แน่นอนที่ผสมผสานกันของความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

2.3.10.2 มุ่งเน้นที่เรื่องสำคัญ

หลักการนี้กำหนดให้องค์กรต้องมุ่งเน้นไปที่ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศที่สำคัญที่สุด ทุก ๆ องค์กรต้องเผชิญกับข้อจำกัดด้านจำนวนบุคลากรและเงินทุนสำหรับการจัดกิจกรรมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ดังนั้นองค์กรต้องมั่นใจว่าได้ใช้ทรัพยากรอย่างมีประสิทธิภาพ ทั้งในด้านการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศและต่อจากนั้น มุ่งเน้นไปที่เรื่องสำคัญเพียง 2-3 เรื่อง กำหนดไว้ดังนี้

(1.) กำหนดเป้าหมายในการรวบรวมข้อมูลเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัย

(2.) กำหนดสินทรัพย์ที่สำคัญที่สุดขององค์กรและเลือกวิธีการรักษาความมั่นคงปลอดภัยสำหรับสินทรัพย์เหล่านั้น

2.3.10.3 การจัดการแบบบูรณาการ

หลักการนี้กำหนดให้นโยบายและกลยุทธ์ด้านความมั่นคงปลอดภัยต้องสอดคล้องกับนโยบายและกลยุทธ์ขององค์กร ในการจัดทำนโยบายขององค์กรในเชิงรุกควรนำประเด็นด้านการดำเนินธุรกิจพิจารณาร่วมกับประเด็นด้านความมั่นคงปลอดภัย เพื่อสร้างความสมดุลระหว่างเป้าหมายทางธุรกิจและความมั่นคงปลอดภัย การจัดการแบบบูรณาการกำหนดไว้ดังนี้

(1.) รวบรวมประเด็นด้านความมั่นคงปลอดภัยไว้ในกระบวนการดำเนินธุรกิจขององค์กร

(2.) พิจารณากลยุทธ์และเป้าหมายทางธุรกิจในการสร้างและปรับปรุงกลยุทธ์และนโยบายความมั่นคงปลอดภัยสารสนเทศ

2.3.11 หลักการและวัฒนธรรมองค์กร

เป็นหลักการที่ช่วยในการสร้างวัฒนธรรมองค์กรที่ที่เอื้อต่อการบริหารความเสี่ยงอย่างมีประสิทธิภาพ

2.3.11.1 การสื่อสารแบบเปิด

การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ไม่สามารถสำเร็จลุล่วงไปโดยปราศจากการสื่อสารแบบเปิดในประเด็นที่เกี่ยวข้องกับความมั่นคงปลอดภัย เราจะไม่สามารถรับรู้

ถึงความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศได้หากไม่มีการสื่อสารเพื่อสร้างการรับรู้จากผู้ทำหน้าที่ตัดสินใจในองค์กร แนวคิดพื้นฐานที่อยู่เบื้องหลังความสำเร็จของโปรแกรมการบริหารความเสี่ยงคือวัฒนธรรมที่ส่งเสริมการสื่อสารแบบเปิดของความเสี่ยงสารสนเทศผ่านการทำงานร่วมกันในกระบวนการประเมิน การสื่อสารแบบเปิดกำหนดไว้ดังนี้

(1.) กิจกรรมการประเมินที่สร้างขึ้นระหว่างกระบวนการ (เช่น workshop)

(2.) ส่งเสริมการแลกเปลี่ยนข้อมูลด้านความมั่นคงปลอดภัยและความเสี่ยงสารสนเทศในทุกระดับขององค์กร

(3.) ใช้กระบวนการฉันทามติที่ให้คุณค่าในสิทธิเสียงของแต่ละคน

2.3.11.2 มุมมองที่กว้างขวาง

หลักการนี้กำหนดให้พนักงานขององค์กรสร้างมุมมองร่วมกันว่าสิ่งใดสำคัญต่อองค์กรมากที่สุด เป็นการนำมุมมองส่วนบุคคลที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศมารวมกันไว้ เพื่อสร้างภาพรวมเป้าหมายความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่องค์กรต้องดำเนินการ มุมมองที่กว้างขวาง กำหนดไว้ดังนี้

(1.) ระบุมุมมองที่หลากหลายของความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่มีอยู่ในองค์กร

(2.) ตรวจสอบความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศภายในบริบทใหญ่ของวัตถุประสงค์ในการดำเนินธุรกิจและภารกิจขององค์กร

2.3.11.3 การทำงานเป็นทีม

ไม่มีบุคคลใดสามารถเข้าใจประเด็นความมั่นคงปลอดภัยสารสนเทศที่องค์กรเผชิญอยู่ได้ด้วยตัวคนเดียว การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศต้องใช้วิธีการแบบสหวิทยาการ รวมทั้งด้านธุรกิจ และมุมมองด้านเทคโนโลยีสารสนเทศ การทำงานเป็นทีมกำหนดไว้ดังนี้

(1.) สร้างทีมทำงานแบบสหวิทยาการเพื่อเป็นผู้นำในการประเมิน

(2.) การรับรู้ถึงมุมมองที่ควรมีเพิ่มในกิจกรรมการประเมิน

(3.) ทำงานร่วมกันเพื่อให้กิจกรรมการปะเมินสำเร็จ

(4.) ใช้พรสวรรค์ ทักษะ และความรู้ของพนักงานให้เป็นประโยชน์

2.4 กรอบการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานที่สำคัญยิ่งยวด (Framework for Improving Critical Infrastructure Cybersecurity)

ความซับซ้อนและการเชื่อมต่อที่เพิ่มมากขึ้นของระบบโครงสร้างพื้นฐานที่สำคัญยิ่งยวด ทำให้มีความเสี่ยงด้านความมั่นคงปลอดภัยของประเทศ เศรษฐกิจ ความปลอดภัยของสาธารณชน สุขภาพ รวมไปถึงด้านการเงินด้วย ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ส่งผลกระทบต่อองค์กรโดยตรง สามารถช่วยเพิ่มผลกำไรและรายได้ และสามารถสร้างความเสียหายให้แก่องค์กรทั้งในด้านความสามารถในการสร้างนวัตกรรม และการรักษาลูกค้า การรักษาความมั่นคงปลอดภัยไซเบอร์จึงเป็นสิ่งสำคัญและเป็นส่วนช่วยเสริมในการบริหารความเสี่ยงขององค์กร

เนื่องจากความกดดันที่เพิ่มขึ้นของภัยคุกคามทั้งจากภายในและภายนอก หน่วยงานที่รับผิดชอบโครงสร้างพื้นฐานที่สำคัญยิ่งยวดจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอและต่อเนื่อง วิธีการนี้จำเป็นต้องดำเนินการโดยไม่คำนึงถึงขนาดขององค์กร ภัยคุกคาม หรือความซับซ้อนในการรักษาความมั่นคงปลอดภัยไซเบอร์ในปัจจุบัน ชุมชนโครงสร้างพื้นฐานที่สำคัญยิ่งยวด รวมไปถึงเจ้าของและผู้ประกอบการภาครัฐและเอกชน และหน่วยงานอื่นที่มีบทบาทในการรักษาความมั่นคงปลอดภัยโครสร้างพื้นฐานแห่งชาติ

ในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ จำเป็นต้องมีความเข้าใจการดำเนินธุรกิจขององค์กร และการพิจารณาด้านความมั่นคงปลอดภัยในการใช้เทคโนโลยีที่เฉพาะเจาะจง เนื่องจากความเสี่ยง การจัดลำดับความสำคัญ และระบบของแต่ละองค์กรมีความเป็นเอกลักษณ์และแตกต่างกัน เครื่องมือและวิธีการที่จะใช้เพื่อให้บรรลุผลตามกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์จึงต้องแตกต่างกัน

ในแต่ละองค์กรมีกระบวนการจัดการด้านความเป็นส่วนตัวและสิทธิเสรีภาพอยู่แล้ว วิธีการของกรอบฯ ถูกออกแบบมาเพื่อเสริมกระบวนการดังกล่าว และเป็นแนวทางในการอำนวยความสะดวกในการจัดการความเสี่ยงด้านข้อมูลที่สอดคล้องกับแนวทางขององค์กรในการจัดการความเสี่ยงในโลกไซเบอร์

กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้จะเสนอกลไกและอนุกรมวิธานทั่วไป (Common Taxonomy) สำหรับองค์กร ดังนี้

(1.) อธิบายถึงการรักษาความมั่นคงปลอดภัยขององค์กรในปัจจุบัน

(2.) อธิบายถึงเป้าหมายหลักในการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร

(3.) ระบุและจัดลำดับความสำคัญในการปรับปุงกระบวนการอย่างต่อเนื่อง

(4.) มีกระบวนการประเมินความคืบหน้าในการก้าวไปสู่เป้าหมาย

(5.) มีการสื่อสารระหว่างผู้มีส่วนได้ส่วนเสีย ทั้งภายในและภายนอกองค์กร เกี่ยวกับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กรอบนี้ไม่ใช่วิธีการที่จะใช้ในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ได้เหมาะสมสำหรับทุกองค์กร เนื่องจากแต่ละองค์กรมีความเสี่ยงที่เฉพาะเจาะจง มีช่องโหว่และภัยคุกคามที่แตกต่างกัน ซึ่งในแต่ละองค์กรก็จะมีกระบวนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อยู่แล้ว ซึ่งกรอบนี้จะช่วยส่งเสริมกระบวนการดังกล่าว โดยภาพรวมของกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ จะแสดงในข้อ 2.4.1

2.4.1 ภาพรวมของกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์

กรอบนี้ใช้สำหรับการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย 3 ส่วนคือ (1) the Framework Core (2) the Framework Implementation Tiers (3) Framework Profiles ในแต่ละส่วนจะช่วยกันเชื่อมต่อระหว่างธุรกิจ การดำเนินงาน และกิจกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้

(1) แกนหลักของกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ (Core Framework) คือชุดกิจกรรมด้านความมั่นคงปลอดภัยไซเบอร์ ผลลัพธ์ที่ต้องการ และการนำข้อมูลอ้างอิงที่มีส่วนเกี่ยวข้องกับ โครงสร้างพื้นฐานที่สำคัญยิ่งยวดมาประยุกต์ใช้ Core แสดงถึงมาตรฐานการอุตสาหกรรม แนวทาง และการสื่อสารด้านกิจกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กร ตั้งแต่ระดับผู้บริหารไปจนถึงระดับปฏิบัติการ Core Framework ประกอบด้วย 5 ฟังก์ชันที่ทำงานพร้อมกันและต่อเนื่อง Identify, Protect, Detect, Respond and Recover เมื่อพิจารณาร่วมกันจะช่วยให้มองเห็นกลยุทธ์ขององค์กรในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในระดับสูง

(2) ระดับการดำเนินการตามกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ (Framework Implementation Tiers “Tier”) ช่วยให้ทราบวิธีการในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร Tiers อธิบายถึงระดับการปฏิบัติตามลักษณะของแต่ละองค์กร ที่กำหนดไว้ในกรอบ เช่น ความเสี่ยงและความตระหนักถึงภัยคุกคาม การทำซ้ำ และการปรับเปลี่ยน

(3) สภาวการณ์ขององค์กรตามกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ (A Framework Profile) แสดงถึง ผลลัพธ์ที่องค์กรเลือกจากหมวดหมู่และหมวดหมู่ย่อยของกรอบโดย

มีพื้นฐานตามความต้องการทางธุรกิจ Profile สามารถแสดงลักษณะของการจัดวางมาตรฐาน แนวทาง และการปฏิบัติสำหรับ Framework Core ในสถานการณ์การดำเนินงานที่เฉพาะเจาะจง Profile สามารถระบุโอกาสในการปรับปรุงการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยการเปรียบเทียบ Current Profile กับ Target Profile ในการพัฒนา Profile องค์กรควรตรวจสอบหมวดหมู่และหมวดหมู่ย่อยทั้งหมด และให้ตัวขับเคลื่อนธุรกิจ/ภารกิจ และการประเมินความสี่ยงเป็นตัวกำหนดว่าสิ่งใดสำคัญที่สุด และบรรจุหมวดหมู่และหมวดย่อยไปใช้ในการจัดการความเสี่ยงขององค์กร Current Profile สามารถช่วยในการจัดลำดับความสำคัญ และใช้เป็นเครื่องมือวัดความก้าวหน้าไปสู่ Target Profile ต่อไปในข้อ 2.4.2 จะกล่าวถึงการบริหารความเสี่ยง และกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์

2.4.2 การบริหารความเสี่ยง และกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์

การจัดการความเสี่ยงเป็นกระบวนการที่ดำเนินการโดยมีการระบุ การประเมิน การรับมือกับความเสี่ยง ในการที่จะจัดการความเสี่ยง องค์กรจะต้องเข้าใจถึงเหตุการณ์ที่เป็นไปได้ว่าจะเกิดขึ้น และผลกระทบอาจเกิดขึ้นด้วย โดยนำข้อมูลนั้นมากำหนดระดับที่ยอมรับได้ของความเสี่ยงเพื่อให้บรรลุวัตถุประสงค์ขององค์กรและสามารถกำหนดระดับความเสี่ยงที่ยอมรับได้ให้ชัดเจนด้วย

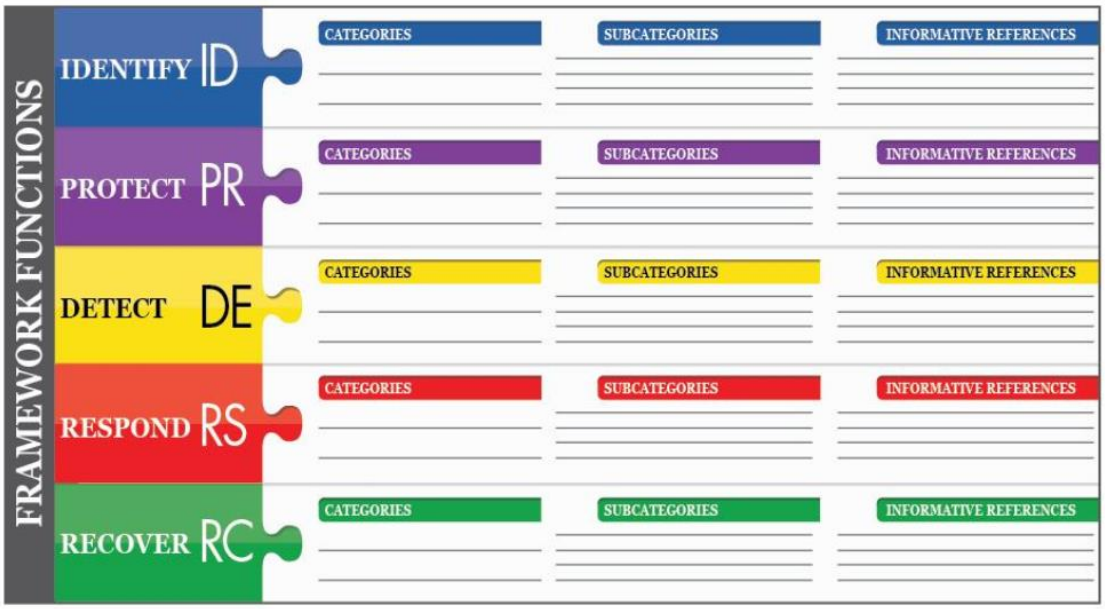
เมื่อสามารถกำหนดระดับความเสี่ยงที่ยอมรับได้แล้ว องค์กรจะสามารถจัดลำดับความสำคัญของกิจกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ได้ กรอบใช้กระบวนการบริหารความเสี่ยงเพื่อให้องค์กรสามารถตัดสินใจในการจัดลำดับความสำคัญเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อช่วยให้องค์กรสามารถกำหนดเป้าหมายหลักในการดำเนินกิจกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้สะท้อนถึงผลลัพธ์ที่ต้องการ ต่อไปในข้อ 2.4.3 จะกล่าวถึงพื้นฐานของกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์

2.4.3 พื้นฐานของกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์

กรอบนี้ใช้ภาษาทั่วไปเพื่อความเข้าใจ การจัดการ และการนำเสนอความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กร สามารถใช้เพื่อช่วยระบุและจัดลำดับความสำคัญสำหรับลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และเป็นเครื่องมือสำหรับการวางนโยบาย การทำธุรกิจ และการใช้เทคโนโลยีในการจัดการความเสี่ยงนั้น สามารถใช้กรอบในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ได้ทั่วทั้งองค์กร หรือใช้ให้เฉพาะสำหรับจุดสำคัญภายในองค์กร

2.4.4 แกนหลักของกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์

แกนหลักของกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ (Framework Core) เป็นชุดกิจกรรมและตัวอย่างในการอ้างอิงเพื่อให้บรรลุตามผลลัพธ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ตั้งไว้ และตัวอย่างในการอ้างอิงเพื่อให้บรรลุถึงผลลัพธ์นั้น Core ประกอบด้วย 4 องค์ประกอบ: ฟังก์ชัน (Functions), หมวดหมู่ (Categories), หมวดหมู่ย่อย (Subcategories), และข้อมูลอ้างอิง (Informative References) ดังภาพประกอบที่ 2.7



ภาพประกอบที่ 2.7 โครงสร้างหลักของกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์

องค์ประกอบหลักของกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ ทำงานร่วมกันดังนี้

2.4.4.1 ฟังก์ชัน (Functions) จะจัดระบบกิจกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นพื้นฐานในระดับสูงสุด Functions ประกอบด้วย Identify, Protect, Detect, Respond, and Recover ช่วยองค์กรในการแสดงถึงการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยการจัดการด้านสารสนเทศ ช่วยในการตัดสินใจด้านการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การรู้จักภัยคุกคาม และปรับปรุงโดยการเรียนรู้จากกิจกรรมที่ผ่านมา

2.4.4.2 หมวดหมู่ (Categories) เป็นส่วนย่อยของ Function ได้แก่ การจัดการสินทรัพย์ มาตรการการจัดการ การควบคุมการเข้าถึง และกระบวนการตรวจจับ

2.4.4.3 หมวดหมู่ย่อย (Subcategory) แบ่งหมวดหมู่ (Category) ไปสู่ผลลัพธ์ที่เฉพาะเจาะจงมากขึ้นของกิจกรรมด้านเทคนิค และ/หรือกิจกรรมด้านการจัดการ ได้แก่ การจัด

หมวดหมู่ของระบบข้อมูลจากภายนอก การปกป้องข้อมูล การตรวจสอบการแจ้งเตือนของระบบตรวจจับ

2.4.4.4 ข้อมูลอ้างอิง (Informative References) คือส่วนเฉพาะของมาตรฐาน แนวทาง และการปฏิบัติ ที่เกี่ยวข้องกับโครงสร้างพื้นฐานที่สำคัญยิ่งยวด ที่แสดงให้เห็นถึงวิธีการที่จะทำผลลัพธ์ให้สำเร็จตามหมวดหมู่ย่อย

แกนหลักของกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ (Framework Core) ทั้ง 5 ฟังก์ชัน ควรดำเนินการควบคุมกับทั้ง 5 Core อย่างต่อเนื่อง เพื่อสร้างวัฒนธรรมในการดำเนินงานในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์แบบยืดหยุ่น

(1.) Identify – พัฒนาความเข้าใจขององค์กรเกี่ยวกับการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ในด้าน คน สินทรัพย์ ข้อมูล และความสามารถ

กิจกรรมในฟังก์ชัน Identify เป็นพื้นฐานในการใช้กรอบอย่างมีประสิทธิภาพ ให้เข้าใจถึงบริบทของการดำเนินธุรกิจ ทรัพยากรที่สนับสนุนฟังก์ชันที่สำคัญ และความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง เพื่อให้องค์กรสามารถมุ่งเน้นและจัดลำดับความสำคัญ ให้สอดคล้องกับกลยุทธ์การบริหารความเสี่ยงและความต้องการทางธุรกิจ ได้แก่ การบริหารสินทรัพย์ สิ่งแวดล้อมทางธุรกิจ ธรรมาภิบาล การประเมินความเสี่ยง และกลยุทธ์การบริหารความเสี่ยง

(2.) Protect – พัฒนาและจัดทำการป้องกันที่เหมาะสมเพื่อให้แน่ใจว่าหน่วยงานที่สำคัญได้รับการปกป้อง

ฟังก์ชัน Protect ช่วยเพิ่มความสามารถในการจำกัดหรือยับยั้งผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ได้แก่ การระบุตัวตนและการควบคุมการเข้าถึง การสร้างความตระหนักและการฝึกอบรม การรักษาความปลอดภัยของข้อมูล กระบวนการและขั้นตอนการปกป้องสารสนเทศ การบำรุงรักษา และเทคโนโลยีด้านการป้องกัน

(3.) Detect – พัฒนาและจัดทำกิจกรรมที่เหมาะสมในการระบุเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้น

ฟังก์ชัน Detect ช่วยให้สามารถตรวจพบเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ได้ทันท่วงที ได้แก่ เหตุการณ์ความผิดปกติ การเฝ้าระวังอย่างต่อเนื่อง และกระบวนการตรวจจับ

(4.) Respond – พัฒนาและจัดทำกิจกรรมที่เหมาะสม เพื่อดำเนินการเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

ฟังก์ชัน Respond ช่วยให้สามารถยับยั้งผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ได้แก่ การวางแผนรับมือ การสื่อสาร การวิเคราะห์ การบรรเทาความเสียหาย และการปรับปรุง

(5.) Recover – พัฒนาและจัดทำกิจกรรมที่เหมาะสมเพื่อวางแผนเตรียมรับมือและกู้คืนการดำเนินงานหรือการให้บริการที่เสียหายจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

ฟังก์ชัน Recover ช่วยให้สามารถกู้คืนการปฏิบัติงานให้กลับเป็นปกติได้ทันท่วงที เพื่อลดผลกระทบที่เกิดจากเหตุการณ์ภัยคุกคามไซเบอร์ ได้แก่ การวางแผนการกู้คืน การปรับปรุง การสื่อสาร

2.4.5 ระดับการดำเนินการตามกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์

ระดับการใช้งานกรอบ (Tier) ช่วยให้ทราบถึงบริบทขององค์กรในการมองภาพความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และวิธีจัดการกับความเสี่ยงนั้น ตั้งแต่ระดับ Partial (Tier 1) ไปจนถึง Adaptive (Tier 4), Tier จะมีการอธิบายถึงแนวปฏิบัติด้านการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เข้มข้นและซับซ้อนมากขึ้น ช่วยในการกำหนดขอบเขตการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์โดยความต้องการในการดำเนินธุรกิจ และบูรณาการใช้กับการบริหารความเสี่ยงโดยรวมขององค์กร

ขั้นตอนการเลือก จะพิจารณาการดำเนินการบริหารความเสี่ยงขององค์กร สภาพแวดล้อมภัยคุกคาม กฎหมายและข้อกำหนดทางกฎหมาย การแบ่งปันข้อมูล วัตถุประสงค์การดำเนินธุรกิจ ข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ของห่วงโซ่อุปทาน และข้อจำกัดขององค์กร องค์กรควรกำหนด Tier ที่ต้องการ และต้องมั่นใจว่าระดับที่เลือกตรงกับเป้าหมายขององค์กร สามารถใช้ดำเนินการ และลดความเสี่ยงของสินทรัพย์และทรัพยากรที่สำคัญ ในระดับที่องค์กรยอมรับได้ องค์กรควรพิจารณาแนวทางจากหน่วยงานภายนอก เช่น หน่วยงานรัฐบาล หรือแหล่งข้อมูลอื่น ๆ เพื่อช่วยในการกำหนดระดับที่ต้องการ โดยนิยามของ Tier เป็นดังนี้

2.4.5.1 ระดับ 1: Partial

กระบวนการบริหารความเสี่ยง – การปฏิบัติการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กร ไม่เป็นระเบียบแบบแผน และการจัดการความเสี่ยงปฏิบัติเฉพาะเมื่อเกิดเหตุการณ์ และในบางครั้งก็ปฏิบัติตามความรู้สึกของผู้ปฏิบัติ การจัดลำดับความสำคัญของกิจกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์อาจจะไม่สอดคล้องกับวัตถุประสงค์ในการบริหารความเสี่ยงขององค์กรรวมถึงไม่สอดคล้องกับสภาพแวดล้อมที่เป็นภัยคุกคาม หรือความต้องการในการดำเนินธุรกิจ

โปรแกรมการจัดการความเสี่ยงแบบบูรณาการ – ระดับความตระหนักในเรื่องความสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กรมีขีดจำกัด การดำเนินการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กรเป็นไปอย่างไม่มีระเบียบ ทำแบบเป็นกรณี ๆ ไป ตามประสบการณ์ที่เคยผ่านมาหรือข้อมูลที่ได้รับจากภายนอก องค์กรอาจไม่มีกระบวนการในการแบ่งปันข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ในองค์กร

ความร่วมมือจากภายนอก – องค์กรไม่เข้าใจถึงบทบาทในระบบนิเวศขนาดใหญ่ที่ต้องพึ่งพาอาศัยซึ่งกันและกัน องค์กรไม่ได้รับความร่วมมือหรือไม่ได้รับข้อมูล (เช่น ความเชี่ยวชาญในการจัดการภัยคุกคาม วิธีปฏิบัติที่ดี เทคโนโลยี) จากหน่วยงานที่เกี่ยวข้อง (เช่น ผู้ซื้อ ซัพพลายเออร์ นักวิจัย รัฐบาล) และไม่ได้ใช้ข้อมูลร่วมกัน องค์กรมักไม่ตระหนักถึงความเสี่ยงด้านไซเบอร์ในห่วงโซ่อุปทานของผลิตภัณฑ์และบริการ

2.4.5.2 ระดับ 2: Risk Informed

กระบวนการบริหารความเสี่ยง – การดำเนินงานด้านบริหารความเสี่ยงที่ได้รับอนุมัติจากผู้บริหาร แต่อาจไม่ได้กำหนดเป็นนโยบายของทั้งองค์กร กิจกรรมการจัดลำดับความสำคัญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และการปกป้องที่จำเป็น จะต้องสอดคล้องกับความเสี่ยงขององค์กร หรือข้อกำหนดในการดำเนินธุรกิจโดยตรง

โปรแกรมการบริหารความเสี่ยงแบบบูรณาการ - มีความตระหนักถึงความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในระดับองค์กร แต่การดำเนินการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กรโดยรวมอาจยังไม่ได้จัดทำ มีการแบ่งปันข้อมูลความมั่นคงปลอดภัยไซเบอร์ภายในองค์กรอย่างไม่เป็นทางการ การพิจารณาด้านความมั่นคงปลอดภัยไซเบอร์ในองค์กรดำเนินการในบางส่วนแต่ไม่ครบทุกระดับในองค์กร มีการประเมินความเสี่ยงด้านไซเบอร์ขององค์กรและการประเมินสินทรัพย์ภายนอก แต่ไม่สามารถทำซ้ำได้

ความร่วมมือจากภายนอก – โดยทั่วไปองค์กรจะเข้าใจถึงบทบาทในระบบนิเวศขนาดใหญ่ในการพึ่งพาอาศัยซึ่งกันและกัน แต่ไม่เข้าใจครบทุกองค์ประกอบ องค์กรได้รับความร่วมมือ ข้อมูลจากหน่วยงานที่เกี่ยวข้อง และสร้างข้อมูลขององค์กรขึ้นมา แต่ไม่แบ่งปันข้อมูลให้หน่วยงานอื่น นอกจากนี้ องค์กรตระหนักถึงความเสี่ยงด้านไซเบอร์ของห่วงโซ่อุปทานของผลิตภัณฑ์และบริการ แต่ไม่ดำเนินการอย่างเป็นทางการและต่อเนื่อง

2.4.5.3 ระดับ 3: Repeatable

กระบวนการบริหารความเสี่ยง – มีแนวปฏิบัติการบริหารความสี่ยงขององค์กรที่ได้รับอนุมัติจากผู้บริหารและจัดทำเป็นนโยบาย การปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ได้รับการอัพเดทอยู่เสมอ โดยมีพื้นฐานมาจากการประยุกต์ใช้กระบวนการบริหารความเสี่ยง

โปรแกรมการบริหารความเสี่ยงแบบบูรณาการ – มีการบริหารความเสี่ยงของทั่วทั้งองค์กร การประกาศนโยบายด้านความเสี่ยง กำหนดกระบวนการและขั้นตอน เตรียมการดำเนินการและตรวจสอบล่วงหน้า มีวิธีการที่สอดคล้องในการรับมือกับความเสี่ยงอย่างมีประสิทธิภาพ บุคลากรมีความรู้และทักษะเพียงพอกับตำแหน่งหน้าที่ความรับผิดชอบ องค์กรมีการเฝ้าระวังความสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของสินทรัพย์องค์กรอย่างถูกวิธี ผู้บริหารด้านความมั่นคงปลอดภัยไซเบอร์และผู้บริหารด้านอื่น ๆ มีการสื่อสารกันเป็นประจำเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ผู้บริหารด้านความมั่นคงปลอดภัยไซเบอร์ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยไซเบอร์ในทุกสายงานขององค์กร

ความร่วมมือจากภายนอก – องค์กรเข้าใจบทบาทในการพึ่งพาอาศัยซึ่งกันและกันในระบบนิเวศขนาดใหญ่ และอาจจะช่วยส่งเสริมความเข้าใจด้านความเสี่ยงแก่หน่วยงานอื่นด้วย ได้รับข้อมูลจากหน่วยงานที่เกี่ยวข้องและนำมาใช้ร่วมกับข้อมูลที่มีภายในองค์กร และแบ่งปันข้อมูลนั้นไปยังหน่วยงานอื่น องค์กรตระหนักถึงความเสี่ยงในห่วงโซ่อุปทานของผลิตภัณฑ์และบริการ นอกจากนี้ยังมีการดำเนินการอย่างเป็นทางการเกี่ยวกับความเสี่ยงเหล่านั้น รวมถึงกลไกต่าง ๆ เช่น ข้อตกลงที่เป็นลายลักษณ์อักษร เพื่อสื่อสารถึงข้อกำหนดพื้นฐาน โครงสร้างการกำกับดูแล (เช่น คณะกรรมการบริหารความเสี่ยง) และนโยบายการดำเนินงานและการเฝ้าระวัง

2.4.5.4 ระดับ 4: Adaptive

กระบวนการบริหารความเสี่ยง – องค์กรสามารถปรับการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์โดยยึดพื้นฐานจากกิจกรรมด้านความมั่นคงปลอดภัยไซเบอร์ที่มีอยู่ในปัจจุบันและในอดีต รวมถึงการเรียนรู้จากบทเรียน และการคาดการณ์ หลังผ่านกระบวนการปรับปรุงอย่าง

ต่อเนื่องผสมผสานกับเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ที่ทันสมัยและการฝึกปฏิบัติ องค์กรจะสามารถปรับตัวให้ทันต่อภัยคุกคามและเทคโนโลยีที่เปลี่ยนแปลง และสามารถรับมือได้ทันท่วงทีด้วยวิธีการที่มีประสิทธิภาพ

โปรแกรมการบริหารความเสี่ยงแบบบูรณาการ – มีวิธีการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ทั่วทั้งองค์กรโดยใช้นโยบาย กระบวนการ และขั้นตอนในการรับทราบข้อมูลเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่มีความเสี่ยง เมื่อต้องทำการตัดสินใจต้องพิจารณาความสัมพันธ์ระหว่างความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และวัตถุประสงค์ขององค์กรอย่างชัดเจน ผู้บริหารต้องติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในบริบทเดียวกับความเสี่ยงด้านการเงินและความเสี่ยงด้านอื่นขององค์กร งบประมาณขององค์กรขึ้นอยู่กับความเข้าใจในสภาพแวดล้อมความเสี่ยงที่มีอยู่และที่คาดการณ์ การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นส่วนหนึ่งของวัฒนธรรมองค์กร และพัฒนามาจากความตระหนักถึงกิจกรรมที่ผ่านมา และการรับรู้ถึงกิจกรรมด้านระบบและเครือข่ายของตนเองอย่างต่อเนื่อง องค์กรสามารถสื่อสารถึงการเปลี่ยนแปลงด้านความเสี่ยงที่มีผลต่อวัตถุประสงค์ในการดำเนินธุรกิจได้อย่างรวดเร็วและมีประสิทธิภาพ

ความร่วมมือจากภายนอก – องค์กรเข้าใจบทบาทการพึ่งพาอาศัยซึ่งกันและกันในระบบนิเวศขนาดใหญ่ และช่วยสร้างความเข้าใจด้านความเสี่ยงแก่หน่วยงานอื่น ได้รับข้อมูล สร้างข้อมูล ทบทวนการจัดลำดับความสำคัญของข้อมูลด้านความเสี่ยงที่ได้รับรายงานการวิเคราะห์อย่างต่อเนื่อง ทันต่อการเปลี่ยนแปลงของภัยคุกคามและเทคโนโลยีที่พัฒนา และแบ่งปันข้อมูลนั้นไปยังหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอก องค์กรใช้ข้อมูลแบบ real-time หรือใกล้เคียงกับ real-time เพื่อทำความเข้าใจและปฏิบัติอย่างต่อเนื่องในห่วงโซ่อุปทานด้านผลิตภัณฑ์และบริการ นอกจากนั้น ยังมีการสื่อสารที่เป็นทางการ เช่น ข้อตกลง และกลไกที่ไม่เป็นทางการเพื่อพัฒนาและรักษาความสัมพันธ์ของห่วงโซ่อุปทานที่เข้มแข็ง

2.4.6 สภาวการณ์ขององค์กรตามกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์

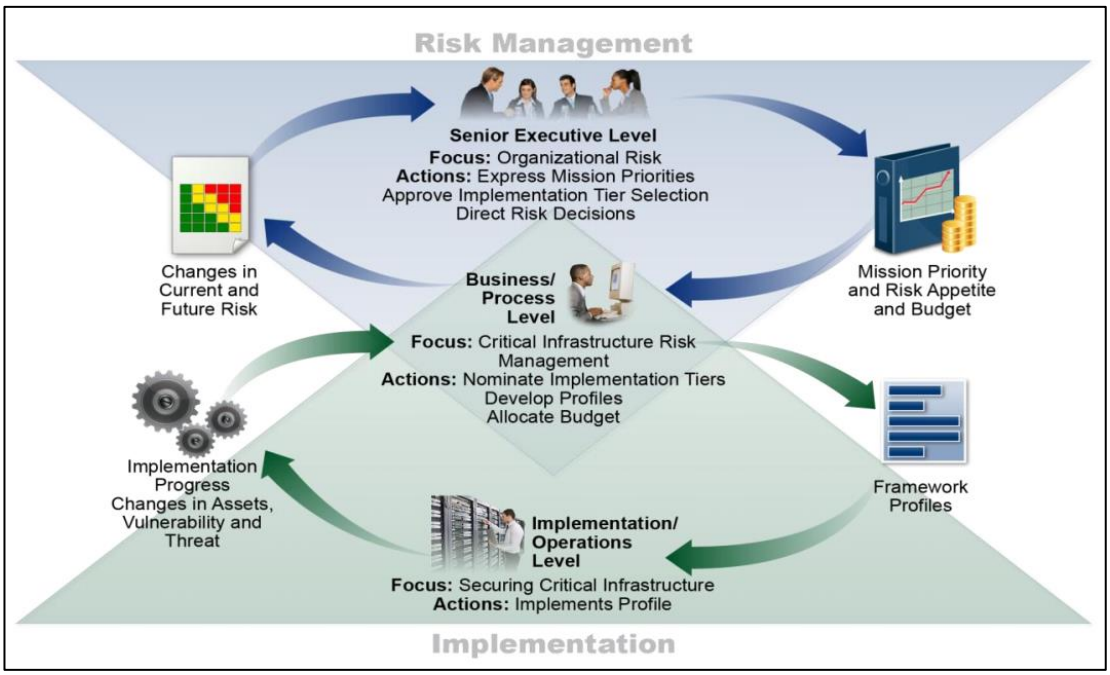
สภาวการณ์ขององค์กรตามกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ (The Framework Profile “Profile”) คือ การจัดวางฟังก์ชัน หมวดหมู่ และหมวดหมู่ย่อย กับความต้องการในการดำเนินธุรกิจ ความต้านทานความเสี่ยง และทรัพยากรขององค์กร Profiles ช่วยให้องค์กรสามารถสร้างแผนงานเพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ที่สอดคล้องกับองค์กร และ

เป้าหมาย การพิจารณาด้านกฎหมาย/ข้อกำหนดทางกฎหมาย และแนวปฏิบัติที่ดีในอุตสาหกรรม และสะท้อนถึงการจัดลำดับความสำคัญในการบริหารความเสี่ยง เนื่องจากความซับซ้อนในการจัดการองค์กร อาจจะเลือกที่จะสร้างหลาย Profiles ให้สอดคล้องกับองค์ประกอบเฉพาะขององค์กร และตระหนักถึงความต้องการขององค์กร

สภาวการณ์ขององค์กรตามกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ (Framework Profiles) สามารถใช้เพื่ออธิบายสถานะปัจจุบัน หรือสถานะเป้าหมายที่ต้องการของกิจกรรมความมั่นคงปลอดภัยไซบอร์โดยเฉพาะ Current Profile บ่งชี้ถึงผลลัพธ์การรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำลังเป็นอยู่ในปัจจุบัน Target Profile บ่งชี้ถึงผลลัพธ์ที่ต้องการจากการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ Profiles สนับสนุนความต้องการในการดำเนินธุรกิจ และช่วยในการสื่อสารความเสี่ยงทั้งภายในและระหว่างองค์กร กรอบนี้ไม่ได้กำหนดต้นแบบ Profiles แต่อนุญาตให้ดำเนินการได้อย่างยืดหยุ่น

2.4.7 ความร่วมมือในการจัดทำกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์

ความร่วมมือในการจัดทำกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ แบ่งเป็น 3 ระดับ (1) ระดับบริหาร (2) ระดับธุรกิจ/กระบวนการ (3) ระดับดำเนินการ/ปฏิบัติการ ดังภาพประกอบที่ 2.8 อธิบายการไหลของสารสนเทศและการตัดสินใจตามระดับภายในองค์กร



ภาพประกอบที่ 2.8 การไหลของสารสนเทศและการตัดสินใจภายในองค์กร

ระดับบริหารจะสื่อสารเกี่ยวกับภารกิจสำคัญ ทรัพยากรที่มีอยู่ และความต้านทานความเสี่ยงโดยรวมของกระบวนการในแต่ละระดับ ระดับธุรกิจ/กระบวนการ ใช้ข้อมูลบรรจุเข้าไปในกระบวนการบริหารความเสี่ยง และรวมมือกับระดับดำเนินการ/ปฏิบัติการ ในการสื่อสารความจำเป็นในการดำเนินธุรกิจ และสร้าง Profile ระดับดำเนินการ/ปฏิบัติการ จะสื่อสารกระบวนการจัดทำ Profile ไปยังระดับธุรกิจ/กระบวนการ ระดับธุรกิจ/กระบวนการใช้ข้อมูลนี้เพื่อประเมินผลกระทบ ระดับธุรกิจ/กระบวนการจัดการรายงานผลลัพธ์ของการประเมินผลกระทบนั้น ไปยังระดับบริหาร เพื่อแจ้งให้ทั่วทั้งองค์กรทราบกระบวนการบริหารความเสี่ยง และไปยังระดับดำเนินการ/ปฏิบัติการ เพื่อสร้างความตระหนักเกี่ยวกับผลกระทบทางธุรกิจ

2.5 งานวิจัยที่เกี่ยวข้อง

Mengmeng Ge et al. (2017) ได้เสนอกรอบสำหรับแบบจำลองกราฟิกและการประเมินความมั่นคงปลอดภัยสำหรับ IoT ซึ่งครอบคลุมใน 5 ด้าน ดังนี้ 1) การประมวลผลข้อมูล 2) การสร้างโมเดลความมั่งคงปลอดภัย 3) การจำลองภาพความมั่นคงปลอดภัย 4) การวิเคราะห์ความมั่นคงปลอดภัย 5) การอัพเดทโมเดล โดยได้พัฒนา IoT Generator เพื่อสร้าง IoT Network ด้านความสามารถในการเข้าถึงข้อมูลเครือข่าย และช่องโหว่ข้อมูลของโหนด, A security generator สร้าง HARM แบบขยายตามเครือข่ายที่กำหนด และ Security Evaluator เพื่อวิเคราะห์ความปลอดภัยของเครือข่ายโดยใช้ตัวชี้วัดความปลอดภัยที่หลากหลาย และได้เสนอการประเมินเครือข่ายตัวอย่าง จำนวน 3 เครือข่าย คือ 1) Smart Home 2) Healthcare Monitoring และ 3) Environment Sensing โดย HARM แบบขยายได้ประมวลเส้นทางการโจมตีที่เป็นไปได้ทั้งหมด และในส่วนของการวิเคราะห์ความปลอดภัย HARM แบบขยายก็ได้คำนวณค่าตัวชี้วัดความปลอดภัยที่เลือกไว้ จากผลการวิเคราะห์ช่วยให้สามารถตัดสินใจในส่วนที่เสี่ยงที่สุดของเครือข่าย เพื่อประเมินประสิทธิภาพของกลไกการป้องกันที่แตกต่างกันและเลือกวิธีการป้องกันเครือข่ายที่มีประสิทธิภาพมากที่สุด เพื่อให้ผลกระทบด้านความเสี่ยงจากภัยคุกคามไซเบอร์ลดน้อยลง

Elisa Bertino (2017) ได้เสนอภาพร่างความเสี่ยงด้านความมั่นคงปลอดภัยและความเป็นส่วนตัวใน IoT และความมั่นคงปลอดภัยด้านแอพพลิเคชันโดเมน รวมทั้งเสนอแผนงานด้านความมั่นคงปลอดภัยใน 3 ด้านดังนี้

1) การควบคุมการเข้าถึง เป็นการรักษาความมั่นคงปลอดภัยขั้นพื้นฐานเมื่อต้องมีการแบ่งปันข้อมูลที่มีความสำคัญกับอุปกรณ์และเครือข่ายอื่น

2) ความมั่นคงปลอดภัยของซอฟต์แวร์และเฟริมแวร์ ซอฟต์แวร์เป็นองค์ประกอบที่สำคัญของ IoT มีการโจมตีหลายครั้งที่ทำให้ซอฟต์แวร์ทำงานผิดพลาด และยังมีการโจมตีโดยอาศัยช่วงการอัพเดทของเฟริมแวร์ด้วย

3) ระบบตรวจจับการบุกรุก ที่เหมาะสมกับ IoT จะต้องได้รับการออกแบบมาเพื่อรองรับการกำหนดค่าที่ยืดหยุ่นในระบบ IoT และที่สำคัญคือต้องตรวจจับการบุกรุกได้โดยที่ไม่ต้องติดตั้งซอฟต์แวร์เพิ่มเติมในอุปกรณ์ IoT

โดยสรุปไว้ว่าการรักษาความมั่งคงปลอดภัยใน IoT เป็นเรื่องที่ท้าทาย เนื่องจากอุปกรณ์แต่ละชนิดมีความหลากหลาย ทั้งในด้านการสื่อสาร โปรโตคอล และซอฟต์แวร์ อุปกรณ์ส่วนใหญ่เป็นระบบปิด เหมาะกับแอพพลิเคชันที่เฉพาะเจาะจง ซึ่งนับเป็นข้อดีในการรักษาความมั่นคงปลอดภัย แต่เมื่ออุปกรณ์ IoT ใช้งานร่วมกับอุปกรณ์อื่น การรักษาความมั่นคงปลอดภัยก็เป็นเรื่องที่ทำได้ยาก

Kui Ren (2017) ได้เสนอว่าอุปกรณ์สมาร์ทโฟนสามารถใช้เป็นได้ทั้งอุปกรณ์ต้นทางในการโจมตีอุปกรณ์ IoT อื่น ๆ และสามารถใช้ในการรักษาความมั่นคงปลอดภัยให้กับอุปกรณ์ IoT อื่น ๆ ได้เช่นกัน โดยได้ทดลองใช้กับเครื่องพิมพ์ 3D และการโจมตีด้วยการปลอมแปลงเสียง

1) การโจมตีเครื่องพิมพ์ 3D โดยผู้บุกรุกสามารถจับสัญญาณและเก็บรวบรวมข้อมูลการสร้างพิมพ์เขียวของเครื่องพิมพ์ได้ ในทางกลับกันก็สามารถใช้สมาร์ทโฟนตรวจจับสัญญาณภาพพิมพ์เขียว เพื่อทำการพิมพ์เองได้ ซึ่งผลการทดลองได้ความแม่นยำกว่า 90%

2) การควบคุมด้วยเสียงมีความเสี่ยงต่อการถูกโจมตีด้วยการปลอมตัวจากการบันทึกเสียงไว้ล่วงหน้า หรือการสังเคราะห์เสียง เพื่อแอบอ้างหรือปลอมตัวเป็นผู้ใช้ที่ถูกต้อง แต่ก็สามารถใช้สมาร์ทโฟนตรวจจับการโจมตีด้วยการปลอมแปลเสียงได้เช่นกัน จากการทดลองสามารถตรวจจับการปลอมแปลงได้ 100% อัตราผิดพลาดเท่ากับ 0%

โดยสรุปว่ายังคงต้องศึกษาบทบาทของสมาร์ทโฟนเพื่อทำความเข้าใจถึงความสามารถและผลกระทบด้านความมั่งคงปลอดภัยสำหรับ IoT ให้มากขึ้นซึ่งนับว่าเป็นงานที่ท้าทายมาก

Tokushi Nakashima (2018) ได้เสนอการใช้งานเทคโนโลยี FinTech และ IoT ว่าไม่ใช่เป็นเพียงเครื่องมือที่จะให้ทำโลกสะดวกสบายขึ้นและไม่ใช่วิธีเพิ่มฟังก์ชันการทำงานของผลิตภัณฑ์ บทบาทของ Fintech และ IoT คือ การปรับปรุงและส่งเสริมให้สังคมพัฒนาขึ้น หรือปรับปรุงวิถีความเป็นอยู่และวิธีการคิดของผู้คน โดยเสนอความสุขและความพึงพอใจที่มากขึ้น

ยกตัวอย่างของ Global Mobility Service Inc. (GMS) ที่ได้ใช้เทคโนโลยี FinTech และ IoT นำมาประยุกต์ใช้กับธุรกิจเช่า/ซื้อรถสามล้อในประเทศฟิลิปปินส์ รถสามล้อเหล่านี้เป็นที่นิยมใน

ประเทศฟิลิปปินส์ ซึ่งผู้ขับขี่รถสามล้อรับจ้างส่วนใหญ่เป็นชนชั้นที่มีรายได้ต่ำ ทำให้ไม่สามารถซื้อรถสามล้อเป็นของตนเองได้ หรือหากรถเสียก็ไม่สามารถเปลี่ยนเป็นคันใหม่ได้ เนื่องจากพวกเขาไม่มีบัญชีธนาคารเพื่อทำการกู้เงิน โดย GMS ได้พัฒนาบริการที่ใช้อุปกรณ์ IoT ซึ่งเรียกว่า Mobility-Cloud Connecting System (MCCS) ซึ่งอนุญาตให้มีการเปิด/ปิดการใช้งานยานยนต์จากระยะไกล นำมาติดตั้งกับรถสามล้อและทำสัญญาเช่าแก่ผู้ขับขี่ โดยชำระเงินเป็นรายสัปดาห์หรือรายเดือน โดยมีสถานบันการเงินเป็นคนกลางในการรับชำระเงินแบบ FinTech ทั้งนี้ บริษัทสามารถรวบรวมข้อมูลการขับขี่ของ ผู้เช่าไว้ได้ด้วย หากผู้เช่าคนใดมีความขยัน ขับขี่รถสามล้อบริการเป็นประจำทุกวัน บริษัทก็จะนำข้อมูลที่ได้มาเพื่อจัดลำดับในการตัดสินใจเสนอสินเชื่อให้

โดยสรุปว่า การใช้ FinTech และ IoT ไม่เพียงเพิ่มประสิทธิภาพของผลิตภัณฑ์และบริการที่มีอยู่ หรือปรับปรุงเทคโนโลยีที่มีอยู่ให้ดีขึ้น แต่ช่วยแก้ปัญหา พัฒนา และตอบสนองความต้องการของสังคมด้วย พร้อมทั้งการใช้ IoT จะช่วยให้สังคมตระหนักถึงการบูรณาการระหว่างสาขาธุรกิจและอุตสาหกรรมที่แตกต่างกันให้สามารถทำงานร่วมกันได้

ชลาธิป ทุมกานนท์ (2560) ได้แสดงถึงศักยภาพของ IoT เมื่อใช้งานระบบประมวลผลบนคลาวด์ โดยได้ยกตัวอย่าง ดังนี้

1) ระบบนำทางใน Google Map บนโทรศัพท์มือถือ ซึ่งเป็นคลาวด์ซอฟต์แวร์ที่สามารถแสดงความหนาแน่นของจารจรได้ โดยใช้โทรศัพท์มือถือแต่ละเครื่องที่เชื่อมต่ออินเทอร์เน็ตเป็นเสมือนตัวตรวจวัดสภาพการจราจร ช่วยให้คลาวด์ของกูเกิ้ลคำนวณความหนาแน่นของสภาพการจราจร และส่งข้อมูลมาแสดงผลหรือคำนวณต่อใน Google Map ที่อยู่บนโทรศัพท์มือถือได้

2) กล้องวงจรปิดสำหรับระบบรักษาความปลอดภัยในบ้าน กล้องวงจรปิดแบบคลาวด์ จะส่งภาพไปบันทึกลงในคลาวด์และติดต่อขอคำสั่งในการควบคุมกล้องจากคลาวด์ (ในกรณีที่ผู้ใช้ส่งคำสั่งควบคุมกล้องมาที่คลาวด์) เมื่อผู้ใช้อยู่นอกบ้านก็สามารถเข้าถึงคลาวด์และดูภาพที่บันทึกได้ และถ้าจะดูภาพสดจากกล้องตัวเดียวกันจากหลายอุปกรณ์พร้อมกัน ก็ไม่ทำให้แบนด์วิธการเชื่อมต่อที่บ้านสูงขึ้นมากไปกว่าการดูด้วยอุปกรณ์เดียวแต่อย่างใด

การประมวลผลบนคลาวด์ช่วยให้ IoT แสดงศักยภาพที่แท้จริงออกมาได้ ไม่ว่าจะเป็นการประมวลผลแบบ real time การรับส่งข้อมูลจำนวนมาก และการรักษาความมั่นคงปลอดภัยของข้อมูล

หยาดพิรุณ นาชัยสินธุ์ (2560) ได้นำยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทยมาใช้ในการวิจัย โดยมีวัตถุประสงค์เพื่อศึกษาความก้าวหน้าทางไซเบอร์ที่มีการ

นำมาใช้เป็นเครื่องมือทางยุทธศาสตร์การก่อการร้ายในประเทศไทย และพัฒนายุทธศาสตร์ต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

ผลการวิจัยพบว่าประเทศไทยมีการตื่นตัวและตระหนักในเรื่องของการก่อการร้ายทางไซเบอร์ มีการจัดตั้งหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ เมื่อเกิดเหตุการณ์ก่อการร้ายในประเทศไทยในขั้นรุนแรงหรือเป็นรูปแบบใหม่ องค์กรด้านความมั่นคงปลอดภัยไซเบอร์ไม่สามารถจัดการได้ เนื่องมาจากปัญหาของโครงสร้างองค์กรที่ต้องปฏิบัติตามสายบังคับบัญชาจากเหนือสุดลงล่าง ต้องรอการอนุมัติปฏิบัติการในการเข้าจัดการปัญหา อำนาจในการตัดสินใจและสั่งการไม่เป็นอิสระ สรุปได้ว่าประเทศไทยให้ความสำคัญต่อการก่อการร้าย โดยมีแนวทางหรือนโยบายของผู้บริหารในการสร้างความตระหนักรู้ต่อภัยการโจมตีทางไซเบอร์ ประเด็นที่สำคัญคือการสร้างนโยบายที่ชัดเจนให้องค์กรดำเนินการไปในทิศทางเดียวกัน ลดระบบอุปถัมภ์ การคอร์รัปชัน สายการบังคับบัญชาที่มีมากเกินไปทำให้บริหารงานยาก หากลดปัญหาเหล่านี้ได้ การดำเนินงานในการต่อต้านการก่อการร้ายก็จะมีประสิทธิภาพมากยิ่งขึ้น

พชรอร เพชรสมุทร และมหศักดิ์ เกตุฉ่ำ (2560) ได้วิจัยเรื่องระบบป้องกันการโจรกรรมรถจักรยานยนต์ โดยใช้เทคนิคการรู้จำใบหน้าผ่านคลาวด์ภายใต้แนวคิดอินเทอร์เน็ตเพื่อทุกสิ่ง มีวัตถุประสงค์เพื่อพัฒนาระบบป้องกันการโจรกรรมรถจักรยานยนต์โดยใช้เทคนิคการรู้จำใบหน้าผ่านคลาวด์ภายใต้แนวคิดอินเทอร์เน็ตเพื่อทุกสิ่งโดยใช้เทคนิคการตรวจจับใบหน้า และการรู้จำใบหน้า โดยการประมวลผ่านบอร์ด Raspberry Pi วัดผลจากการนำใบหน้าบุคคลที่รับจากกล้องมาทำการเปรียบเทียบภาพใบหน้าบุคคลที่เป็นเจ้าของรถจักรยานยนต์จากฐานข้อมูลบนคลาวด์ โดยใช้เทคนิค SIFT (Scale Invariant Feature Transform) ถ้าทำการเปรียบเทียบใบหน้าบุคคลทั้งสองภาพแล้วว่ามีความคล้ายคลึงกัน จะไม่ทำการส่งแจ้งเตือนใด ๆ แต่หากภาพใบหน้าบุคคลที่รับจากกล้องนั้นไม่ตรงกัน ระบบจะทำการแจ้งเตือนบนแอปพลิเคชันผ่านระบบเรือข่ายอินเทอร์เน็ต 3G โดยใช้อุปกรณ์ 3G Shield และ GPS Module เพื่อติดตามรถจักรยานยนต์ โดยส่งเป็นภาพใบหน้าบุคคลที่รับจากกล้อง และบอกตำแหน่งที่ตั้งของรถจักรยานยนต์ ณ ปัจจุบันทันที ซึ่งจากการทดสอบระบบอุปกรณ์ และแอปพลิเคชันสามารถทำการแจ้งเตือน บอกตำแหน่งของรถจักรยานยนต์และภาพที่รับเข้ามาจากกล้องได้อย่างแม่นยำ ช่วยเพิ่มประสิทธิภาพในการป้องกันการโจรกรรมรถจักรยานยนต์ และสามารถนำไปใช้ได้จริง

อรพรรณ แซ่ตั้ง และคณะ (2560) ได้วิจัยเรื่องการออกแบบโรงเรือนสำหรับควบคุมอุณหภูมิความชื้น โดยใช้เทคนิคอินเทอร์เน็ตของสรรพสิ่ง เพื่อส่งเสริมการเพาะเลี้ยงเห็ดแครง โดย

มีวัตถุประสงค์เพื่อ 1) การออกแบบโรงเรือนสำหรับควบคุมอุณหภูมิและความชื้น โดยใช้เทคโนโลยีอินเทอร์เน็ตของสรรพสิ่ง และ 2) ประเมินผลการออกแบบโรงเรือนสำหรับควบคุมอุณหภูมิและความชื้น โดยใช้เทคโนโลยีอินเทอร์เน็ตของสรรพสิ่ง

ปัจจุบันมีการพัฒนาอุปกรณ์ต่าง ๆ ให้สามารถให้สามารถทำงานบนแนวคิดของอินเทอร์เน็ตของสรรพสิ่งเพิ่มมากขึ้น ผู้วิจัยจึงมีแนวคิดในการออกแบบโรงเรือนสำหรับควบคุมอุณหภูมิและความชื้น โดยใช้เทคโนโลยีอินเทอร์เน็ตของสรรพสิ่ง สำหรับเป็นโรงเรือนต้นแบบในการศึกษาและนำไปต่อยอดการเพาะเลี้ยงเห็ดแครงต่อไป ซึ่งผลการวิจัยพบว่า 1) การออกแบบโรงเรือนแบ่งออกเป็น 3 ส่วน ประกอบด้วย 1.1) การออกแบบภายนอกโรงเรือนสำหรับควบคุมอุณหภูมิและความชื้น 1.2) การออกแบบภายในโรงเรือนสำหรับควบคุมอุณหภูมิและความชื้น และ 1.3) การออกแบบโรงเรือนสำหรับควบคุมอุณหภูมิและความชื้น ในส่วนของห้องควบคุม และห้องเก็บพลังงานแสงอาทิตย์ 2) ความคิดเห็นของการออกแบบโรงเรือน ภาพรวมอยู่ในระดับมาก ("$\bar{X}$" = 4.40, SD = 0.63) และ 3) ความเหมาะสมของการออกแบบโรงเรือน ภาพรวมอยู่ในระดับมาก ("$\bar{X}$" = 3.90, SD = 0.57) แสดงว่าสามารถนำผลการออกแบบดังกล่าวไปประยุกต์ใช้ในการจัดสร้างโรงเรือนสำหรับเพาะเลี้ยงเห็ดแครงได้อย่างเหมาะสม

ขวัญชนก ศรีมูล และคณะ (2560) ได้วิจัยเรื่อง การศึกษาปรียบเทียบ NETPIE กับแพลตฟอร์ม Internet of Things อื่น ได้แก่ Anto, AWS IoT (Amazon), Azure IoT Hub (Microsoft), Blynk, Firebase Realtime Database (Google) และ IBM Watson Internet of Things (IBM Bluemix) เพื่อให้เห็นความแตกต่างของแต่ละแพลตฟอร์มและสามารถเลือกใช้ได้อย่างเหมาะสม เนื่องจากผู้ให้บริการแพลตฟอร์มสำหรับการสื่อสารเชื่อมโยงอุปกรณ์ IoT เข้าด้วยกันและให้บริการ API เพื่ออำนวยความสะดวกต่อนักพัฒนาก็มีหลากหลายเช่นกัน แต่ละบริการก็มีจุดเด่นและบริการที่แตกต่างกันไป เพื่อที่นักพัฒนาจะสามารถเลือกใช้บริการได้เหมาะสมกับงานและความต้องการของตน การศึกษาจุดเด่นและจุดด้อยของแต่ละบริการของแพลตฟอร์มต่าง ๆ จึงเป็นประโยชน์อย่างยิ่ง ซึ่งผลการวิจัยพบว่าหากจะนำ Internet of Things Platform ไปใช้งานจริงในการพัฒนานั้น ควรเลือกจากคุณสมบัติให้เหมาะสมตามการใช้งานเป็นหลัก

โอฬาร เชี่ยวชาญ และอนุกิจ เสาร์แก้ว (2560) ได้วิจัยเรื่อง การบูรณาการประยุกต์ใช้ RFID (Radio Frequency Identification) และ IoT (Internet of thing) ผ่านระบบคลาวด์ (Cloud Computing) สำหรับการจัดการโลจิสติกส์ โดยบูรณาการประยุกต์ใช้ระบบ RFID และ IoT กับรถขนถ่านหินลิกไนต์ในเหมืองการไฟฟ้าฝ่ายผลิตแม่เมาะ จังหวัดลำปาง ผ่านระบบ Private cloud

computing ของการไฟฟ้า แม่เมาะ เพื่อลดความผิดพลาดในการตรวจสอบจำนวนเที่ยวรถขนถ่านหินลิกไนต์แทนการนับด้วยคน และสามารถดูข้อมูลผ่านคอมพิวเตอร์หรือโทรศัพท์มือถือได้แบบ real-time โดยอุปกรณ์ที่ใช้ในการวิจัย ได้แก่ RFID Reader, UHF passive RFID tag, Arduino Mega 2560 + Ethernet Shield, ภาษา PHP, JSON, Node.JS และ MariaDB เป็นระบบฐานข้อมูล และโปรโตคอลที่ใช้ในการส่งข้อมูลคือ MQTT และได้ทำการติดตั้ง UHF passive Tag กับรถขนถ่านหินจำนวน 27 คัน และติดตั้งเครื่องอ่าน RFID 1 จุดที่ตำแหน่งเครื่องบดถ่านหินลิกไนต์ที่ 3 และระบบนี้ใช้งานมาประมาณ 1 ปี ตั้งแต่ต้นปี 2558 ถึง 2559 ผลการวิจัยพบว่าระบบ RFID และ IoT ที่พัฒนาขึ้นสามารถอ่านค่าและนับจำนวนรถขนถ่านฟินลิกไนต์ได้ถูกต้องและข้อมูลสามารถส่งขึ้นระบบ Cloud และดูข้อมูลผ่านคอมพิวเตอร์และอุปกรณ์โทรศัพท์มือถือได้

ปริญญา หอมเอนก (2558) ได้วิเคราะห์กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ระดับโลก “NIST’s Framework for Improving Critical Infrastructure Cybersecurity” โดยได้สรุปว่า กรอบการดำเนินงาน Cybersecurity Framework นี้ สามารถนำมาใช้ในองค์กรทั่วไปที่ไม่ได้จัดอยู่ในโครงสร้างพื้นฐานสำคัญ และสามารถนำมาประยุกต์ใช้โดยไม่จำเป็นต้องใช้แทนประบวนการบริหารความเสี่ยงที่มีอยู่ แต่ให้เป็นส่วนหนึ่งหรือใช้ร่วมกับกระบวนการที่องค์กรมีอยู่ เพื่อใช้ในการระบุ ประเมิน และจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้ กรอบการดำเนินงาน Cybersecurity Framework มีรูปแบบวิธีการและแนวคิดเพื่อการนำมาใช้ในลักษณะที่ไม่แตกต่างจากแนวทางการดำเนินงานตามแนวคิด GRC (การกำกับดูแลที่ดี การบริหารความเสี่ยงและการปฏิบัติตามกฎระเบียบ) ดังนี้

1) ทบทวนแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์

2) จัดทำหรือปรับปรุงแผนงานด้านความมั่นคงปลอดภัยไซเบอร์ โดยมีลำดับขั้นตอนสอดคล้องตามกระบวนการบริหารความเสี่ยงได้ การจัดลำดับวัตถุประสงค์และขอบเขตที่จะดำเนินการ การระบุปัจจัยเสี่ยง การจัดทำสถานภาพปัจจุบัน (ตามกลุ่มงานและกลุ่มงานย่อยของผลลัพธ์ด้านความมั่นคงปลอดภัยไซเบอร์) การประเมินความเสี่ยง การจัดทำสถานภาพเป้าหมาย การประเมินวิเคราะห์ และการดำเนินแผนงาน

3) สื่อสารข้อกำหนดความต้องด้านความมั่นคงปลอดภัยไซเบอร์กับผู้มีส่วนได้ส่วนเสีย

4) ระบุโอกาสในการจัดทำหรือทบทวนมาตรฐานและแนวปฏิบัติที่อ้างอิง

5) พิจารณาวิธีการเพื่อคุ้มครองสิทธิเสรีภาพและความเป็นส่วนตัว

นอกจากนี้ โครงสร้างหลักของกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญ (Framework Core) ตามกรอบการดำเนินงาน Cybersecurity Framework นี้ ยังสามารถแบ่งรายละเอียดลงไปในแต่ละหัวข้อของทั้ง 5 Function เพื่อเชื่อมโยงข้อมูลอ้างอิง (Informative reference) ซึ่งได้แก่ มาตรฐาน แนวปฏิบัติ หรือข้อกำหนดอื่น ๆ ที่สามารถนำมาประยุกต์ใช้ในแต่ละ Function โดยไม่เพียงครอบคลุมการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์สำหรับเทคโนโลยีสารสนเทศ แต่มุ่งเน้นที่ระบบควบคุมอุตสาหกรรม (Industrial Control System: ICS) ซึ่งมีผลกระทบในวงกว้างมากกว่า ทำให้ผู้ใช้ในกลุ่มหน่วยงานระบบโครงสร้างพื้นฐานสำคัญจะได้รับประโยชน์อย่างเต็มที่ในการใช้กรอบการดำเนินงาน Cybersecurity Framework นี้

บทที่ 3
วิธีดำเนินการวิจัย

การวิจัยครั้งนี้ เพื่อพัฒนากรอบการักษาความมั่นคงปลอดภัยทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง โดยการศึกษาและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่มีผลอินเทอร์เน็ตประสานสรรพสิ่ง ด้วยแอปพลิเคชันระบบประเมินความเสี่ยงด้านภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง ซึ่งผู้วิจัยได้ดำเนินการตามลำดับขั้นตอน ดังนี้

3.1 รูปแบบการวิจัย

3.2 ประชากรและกลุ่มตัวอย่าง

3.3 ขั้นตอนการดำเนินงานวิจัย

3.4 เครื่องมือการวิจัย

3.5 การรวบรวมข้อมูล

3.6 สถิติที่ใช้ในการวิเคราะห์ข้อมูล

3.7 ระยะเวลาดำเนินการ

3.1 รูปแบบการวิจัย

3.1.1 ศึกษาเอกสารและงานวิจัยที่เกี่ยวข้องกับอินเทอร์เน็ตประสานสรรพสิ่ง ความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์

3.1.2 วิเคราะห์ความเสี่ยงและภัยคุกคามทางไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่งจากการสัมภาษณ์เชิงลึกผู้เชี่ยวชาญ และแบบสอบถามปลายปิด

3.1.3 ทำการวิเคราะห์และออกแบบแอปพลิเคชันระบบประเมินความเสี่ยงด้านภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง ตามหลักการ SDLC

3.1.4 จัดทำกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง โดยอ้างอิงจากกรอบการรักษาความมั่นคงปลอดภัยของจาก สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology: NIST)

3.1.5 ทำการประเมินกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง โดยผู้เชี่ยวชาญให้คำปรึกษาและแนะนำ

3.1.6 ปรับปรุง แก้ไข และพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง ตามคำแนะนำของผู้เชี่ยวชาญ

3.2 ประชากรและกลุ่มตัวอย่าง

ประชากรที่ใช้สำหรับการวิจัยเชิงคุณภาพ คือ ผู้เชี่ยวชาญด้านอินเทอร์เน็ตประสานสรรพสิ่ง จำนวน 7 คน

ประชากรที่ใช้เป็นกรณีศึกษาสำหรับการวิจัยเชิงปริมาณ คือ บุคลากรของกองวิศวกรรมและบริการ การไฟฟ้าส่วนภูมิภาค เขต 1 (ภาคใต้) จังหวัดเพชรบุรี จำนวน 40 คน โดยเป็นผู้ที่ทำงานเกี่ยวข้องกับการใช้อุปกรณ์อินเทอร์เน็ตประสานสรรพสิ่ง

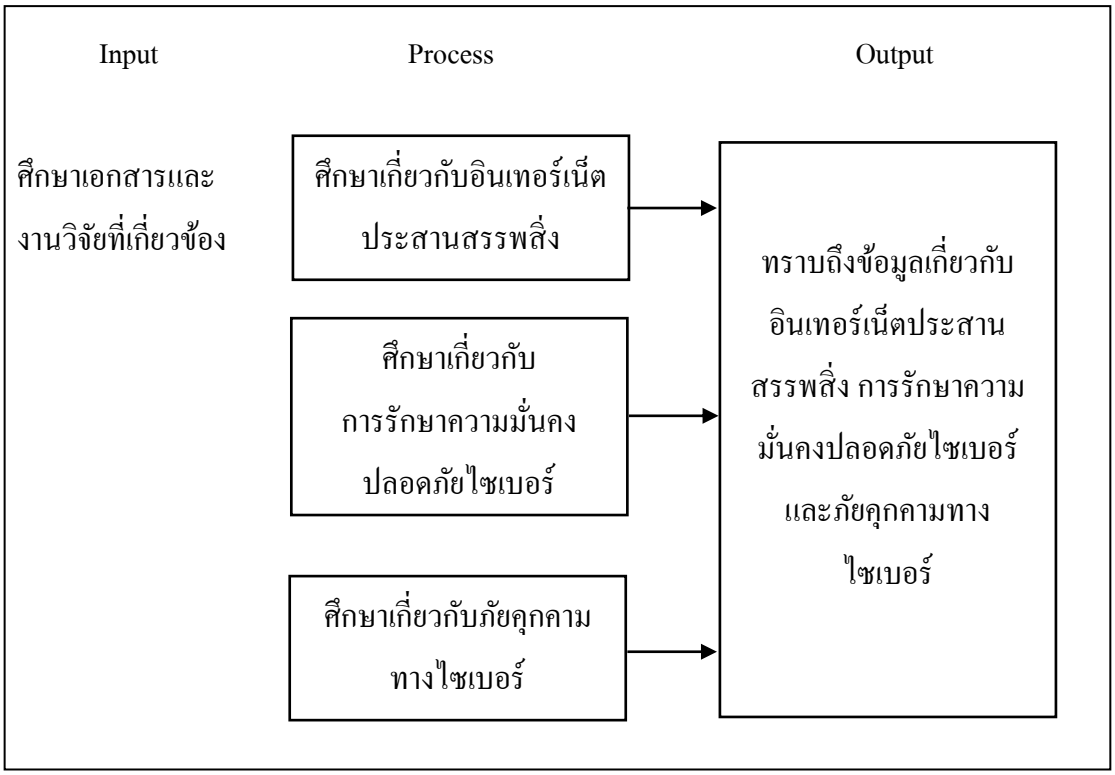
$$n = \frac{N}{1 + N(e)^2}$$

n	คือ	จำนวนของกลุ่มตัวอย่างที่ระดับความเชื่อมั่นที่ 95%
N	คือ	จำนวนรวมทั้งหมดของประชากรที่ใช้ในการศึกษา
e	คือ	ค่าเปอร์เซ็นต์ความคลาดเคลื่อนจากการสุ่มตัวอย่าง (เท่ากับ 0.05)

3.3 ขั้นตอนการดำเนินงานวิจัย

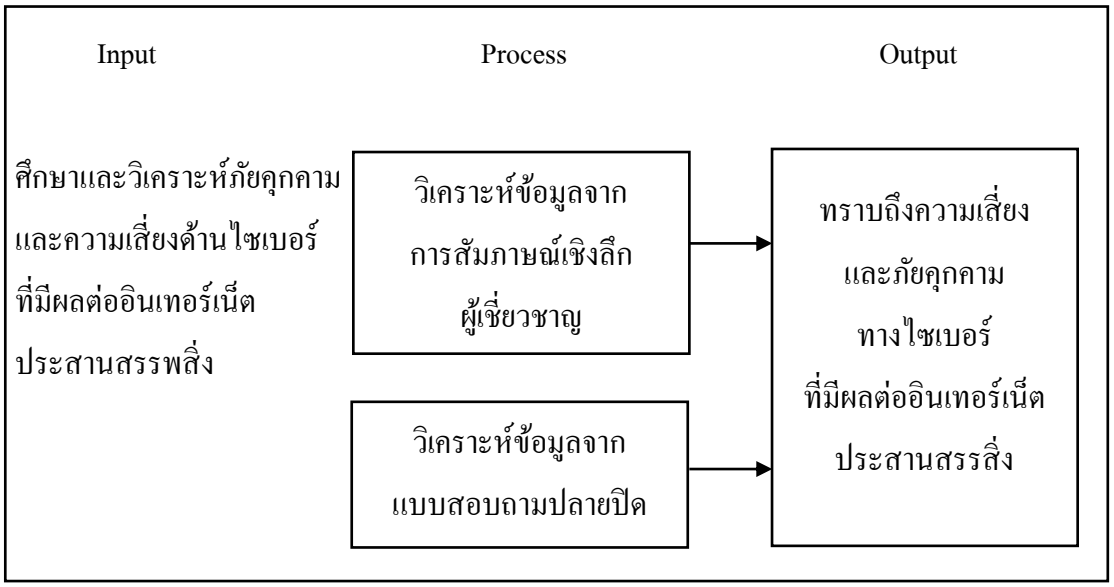
3.3.1 ศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง โดยผู้วิจัยได้ศึกษาเอกสารเกี่ยวกับกับอินเทอร์เน็ตประสานสรรพสิ่ง (Internet of things) มาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Systems: ISO 27001:2013) การประเมินการปฏิบัติการเกี่ยวกับช่องโหว่และสินทรัพย์ ภัยคุกคามที่สำคัญยิ่งยวด (Operationally Critical Threat, Asset and Vulnerability Evaluation: OCTAVE) และกรอบการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานที่สำคัญยิ่งยวด (Framework for Improving Critical

Infrastructure Cybersecurity) รวมถึงศึกษางานวิจัยที่เกี่ยวข้องด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และการประยุกต์ใช้อินเทอร์เน็ตประสานสรรพสิ่งในการดำเนินงานด้านต่าง ๆ ดังภาพประกอบที่ 3.1



ภาพประกอบที่ 3.1 ขั้นตอนการศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง

3.3.2 ทำการศึกษาและวิเคราะห์ภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง โดยการสัมภาษณ์เชิงลึกผู้เชี่ยวชาญด้านอินเทอร์เน็ตปะสานสรรพสิ่ง และใช้แบบสอบถามปลายปิดโดยเป็นกรณีศึกษาของบุคลากรในกองวิศวกรรมและบริการ การไฟฟ้าส่วนภูมิภาค เขต 1 (ภาคใต้) จังหวัดเพชรบุรี จำนวน 40 คน ดังภาพประกอบที่ 3.2



ภาพประกอบที่ 3.2 ขั้นตอนการศึกษาและวิเคราะห์ภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง

3.3.2.1 หัวข้อในการวิจัยเชิงคุณภาพ สำหรับสัมภาษณ์เชิงลึกผู้เชี่ยวชาญด้านอินเทอร์เน็ตประสานสรรพสิ่ง มีดังนี้

ข้อที่ 1 ความสำคัญของอินเทอร์เน็ตประสานสรรพสิ่ง

ข้อที่ 2 ความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง

ข้อที่ 3 ภัยคุกคามด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง

ข้อที่ 4 ความเป็นไปได้ในการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง

ข้อที่ 5 การพัฒนาเตรียมบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง

ข้อที่ 6 ความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง ในภาพรวม

ข้อที่ 7 การเตรียมความพร้อมเพื่อรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง

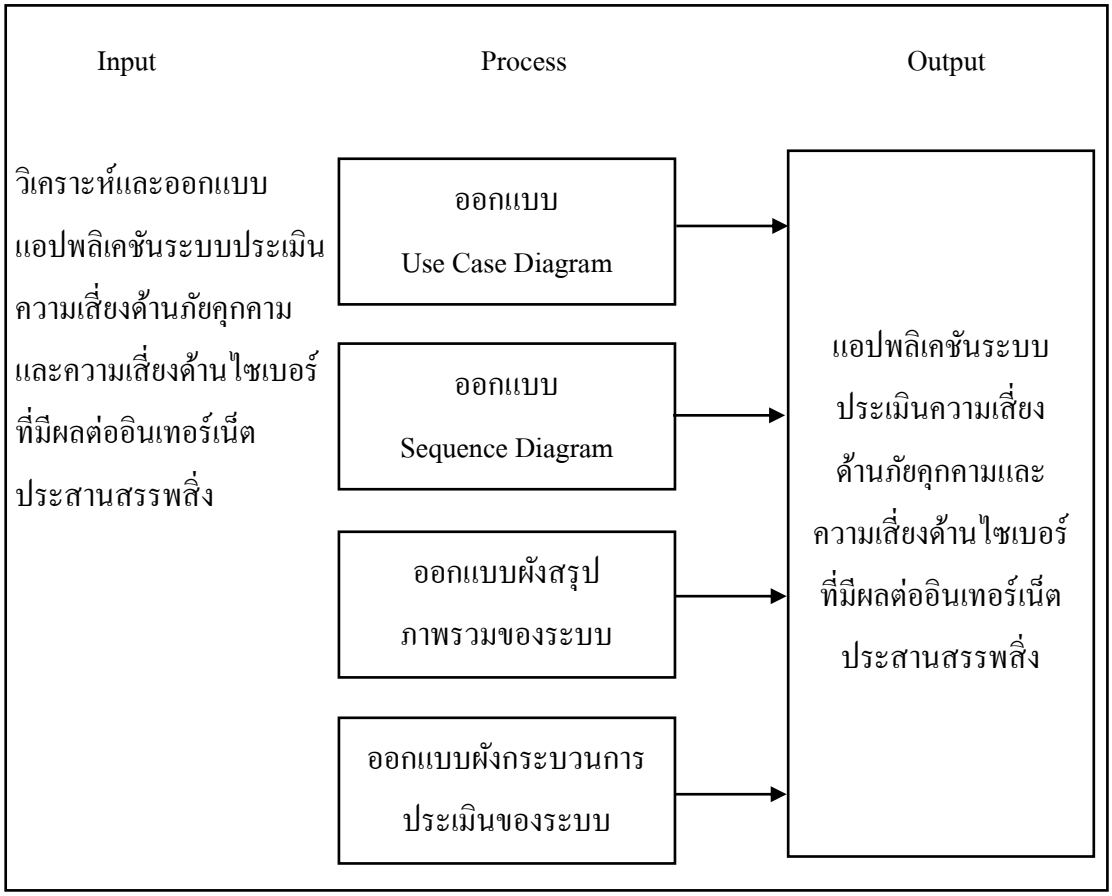
3.3.2.2 แบบสอบถามปลายปิดสำหรับการวิจัยเชิงปริมาณ อ้างอิงจากกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology: NIST) ซึ่งแบ่งเป็น 5 ด้าน ดังนี้

1. การกำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์ (Identify)
2. การปกป้องดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (Protect)
3. การตรวจพบเหตุภัยคุกคามทางไซเบอร์ (Detect)
4. การรับมือภัยคุกคามทางไซเบอร์ (Respond)
5. การกู้คืนข้อมูลหลังเหตุภัยคุกคามไซเบอร์ (Recover)

การวิเคราะห์ความเสี่ยงภัยคุกคามทางไซเบอร์ แบ่งเป็น 5 ระดับ ดังนี้

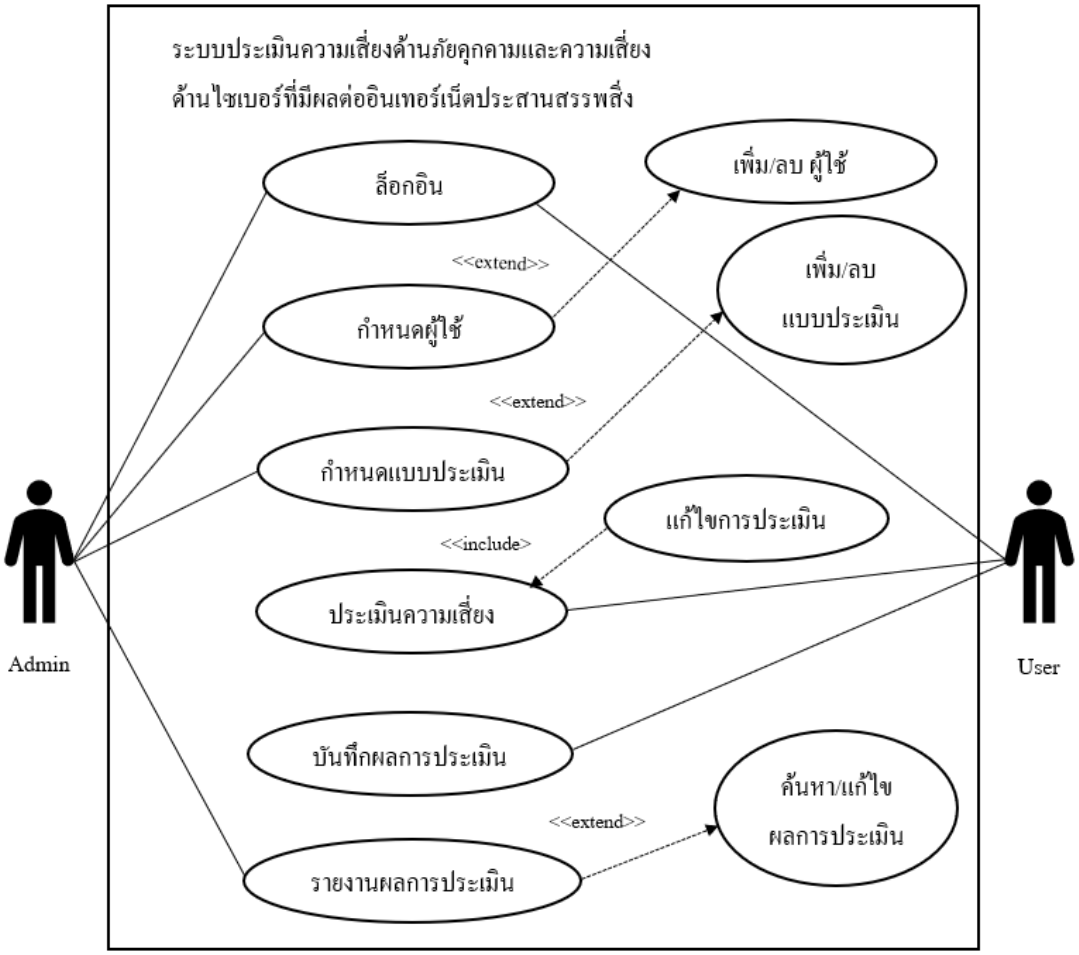
5	หมายถึง	มีความเสี่ยงมากที่สุด
4	หมายถึง	มีความเสี่ยงมาก
3	หมายถึง	มีความเสี่ยงปานกลาง
2	หมายถึง	มีความเสี่ยงน้อย
1	หมายถึง	มีความเสี่ยงน้อยที่สุด

3.3.3 ทำการวิเคราะห์และออกแบบแอปพลิเคชันระบบประเมินความเสี่ยงด้านภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง โดยใช้หลักการของ Use Case Diagram Sequence Diagram ผังภาพรวม และผังกระบวนการ ดังภาพประกอบที่ 3.3



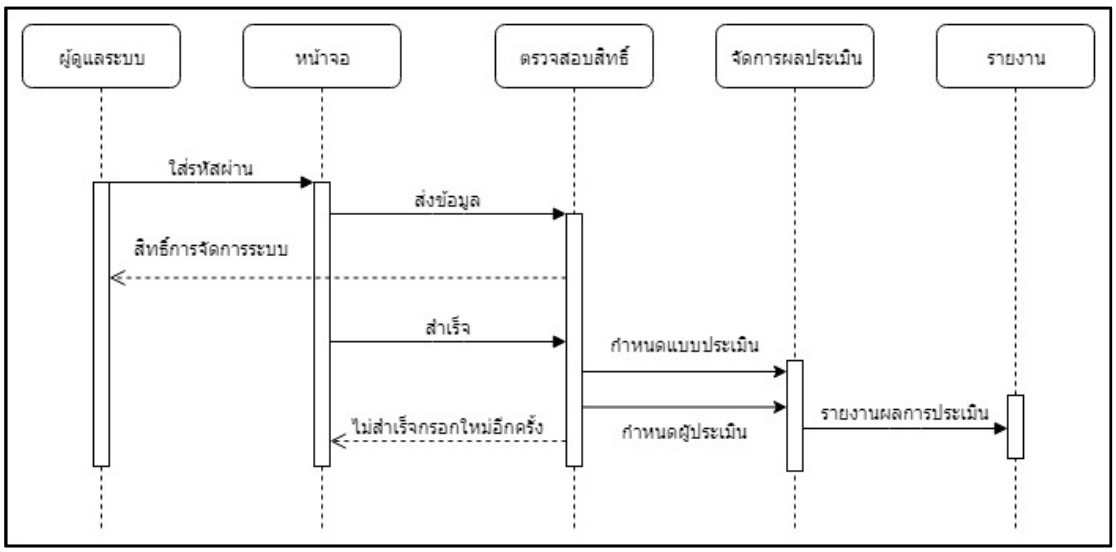
ภาพประกอบที่ 3.3 ขั้นตอนการพัฒนาแอปพลิเคชันระบบประเมินความเสี่ยงด้านภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง

3.3.3.1 ออกแบบระบบเชิงวัตถุตามหลักการของ Use Case Diagram เพื่อหาความเหมาะสมในการพัฒนาระบบสำหรับการใช้งานจริง ดังภาพประกอบที่ 3.4



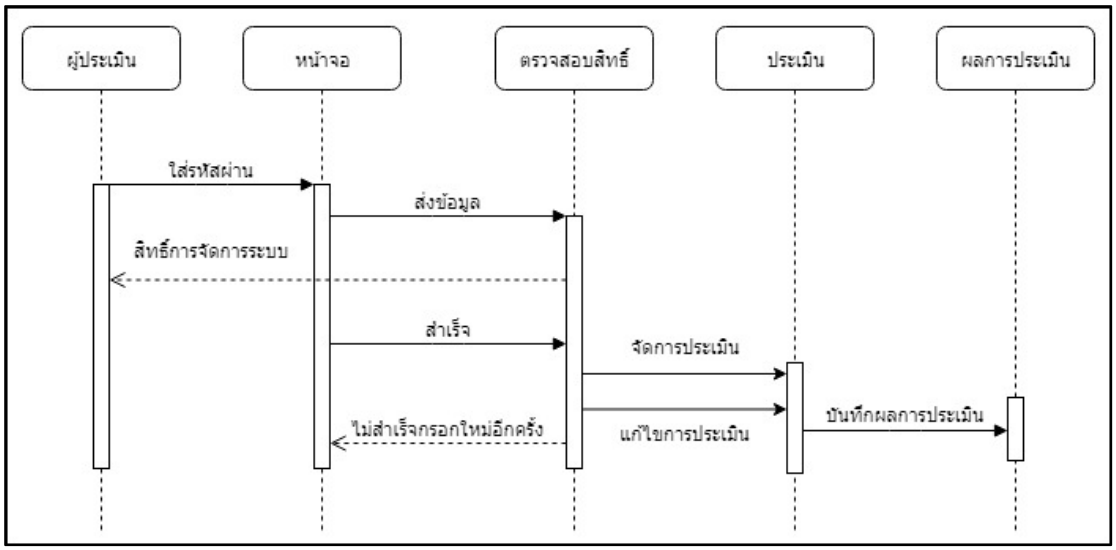
ภาพประกอบที่ 3.4 แสดงแผนภาพ Use Case Diagram ของระบบประเมินความเสี่ยงด้านภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง

3.3.3.2 การจัดการข้อมูลระบบประเมินความเสี่ยงภัยคุกคามทางไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง มีการทำงานดังนี้ ผู้ดูแลระบบ หน้าจอการทำงาน ตรวจสอบสิทธิ์ จัดการผลการประเมิน รายงานผลการประเมิน ดังภาพประกอบที่ 3.5



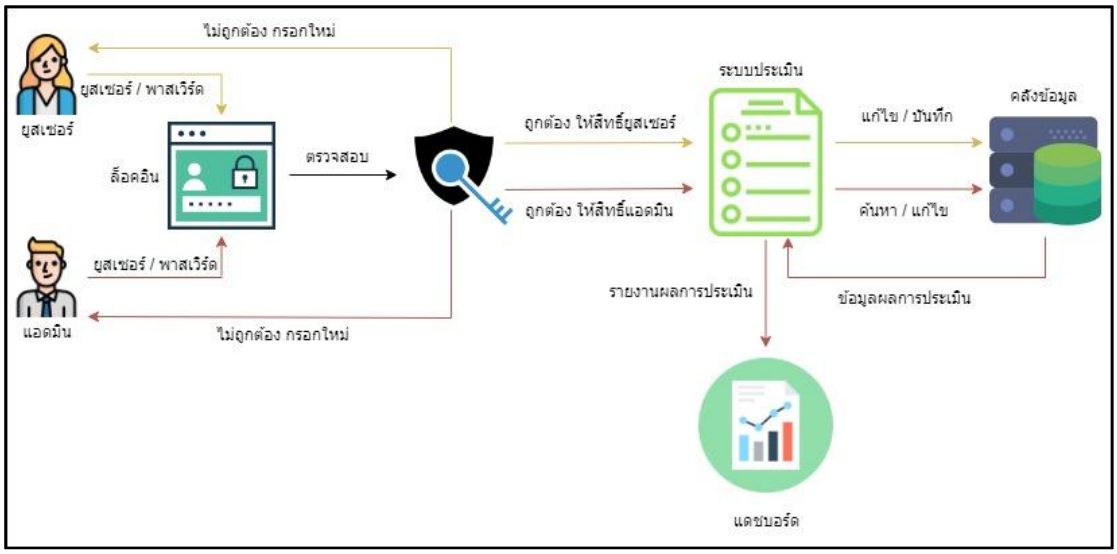
ภาพประกอบที่ 3.5 Sequence Diagram ของผู้ดูแลระบบ

3.3.3.3 การประเมินความเสี่ยงภัยคุกคามทางไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง มีการทำงานดังนี้ ผู้ประเมิน หน้าจอการทำงาน ตรวจสอบสิทธิ์ ประเมินความเสี่ยง บันทึกผลการประเมิน ดังภาพประกอบที่ 3.6



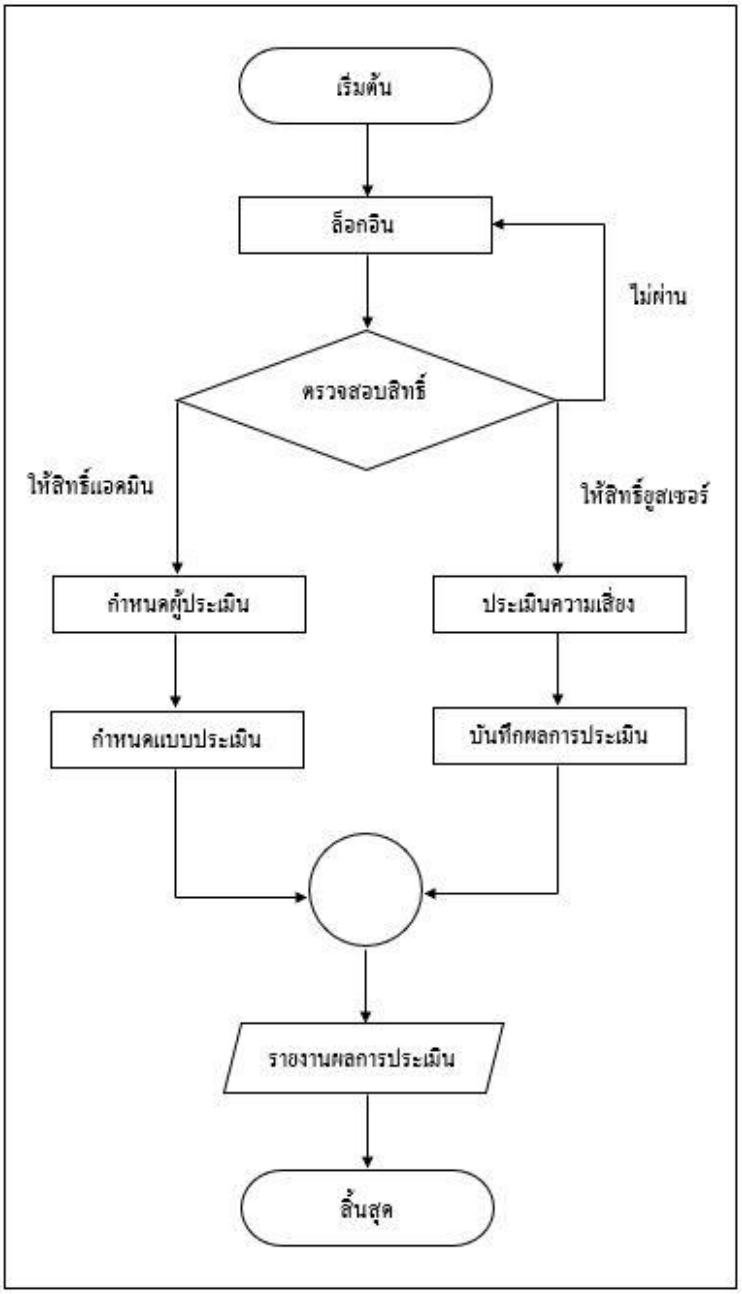
ภาพประกอบที่ 3.6 Sequence Diagram ของผู้ประเมิน

3.3.3.4 สรุปภาพรวมของระบบการประเมินความเสี่ยงภัยคุกคามไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง ดังภาพประกอบที่ 3.7



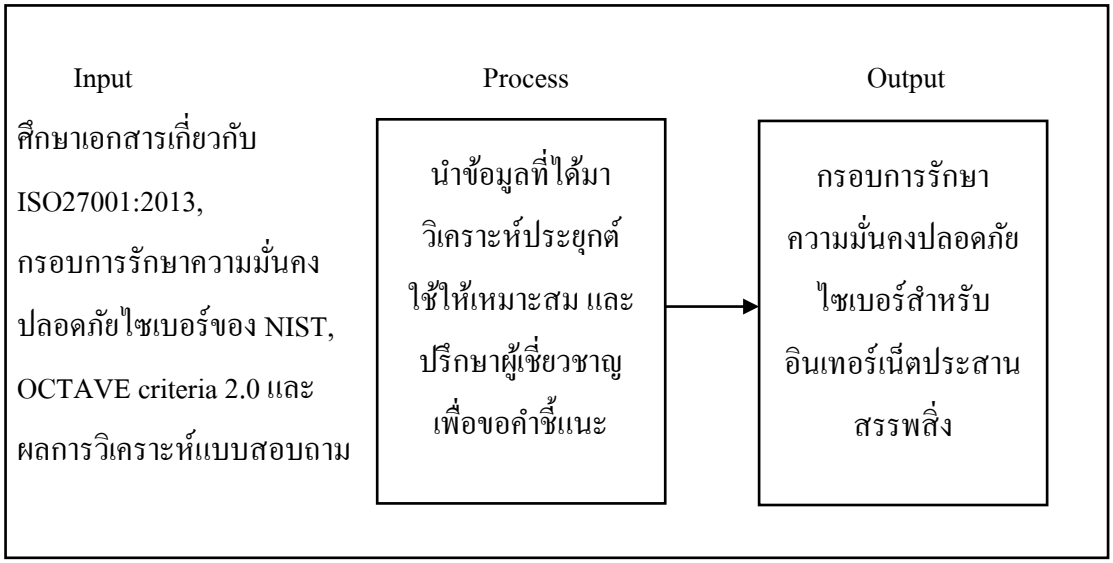
ภาพประกอบที่ 3.7 ผังสรุปภาพรวมของระบบ

3.3.3.5 ผังกระบวนการประเมินของแอปพลิเคชันระบบประเมินความเสี่ยงด้านภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง ดังภาพประกอบที่ 3.8



ภาพประกอบที่ 3.8 ผังกระบวนการประเมินของแอปพลิเคชันระบบประเมินความเสี่ยงด้านภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง

3.3.4 ขั้นตอนพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง ดังภาพประกอบที่ 3.9



ภาพประกอบที่ 3.9 ขั้นตอนการพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง

3.4 เครื่องมือที่ใช้ในการวิจัย

3.4.1 เครื่องมือที่ใช้ในการพัฒนาระบบ

3.4.1.1 ฮาร์ดแวร์ที่ใช้ในการพัฒนาระบบ ประกอบด้วย

- คอมพิวเตอร์ Notebook
- ซีพียู Intel core i5-7200U
- ฮาร์ดดิสก์ความจุ 128 GB และ 1 TB
- หน่วยความจำ 4 GB
- การแสดงผล NVIDIA GEFORCE GT940X

3.4.1.2 ซอฟต์แวร์ที่ใช้ในการพัฒนาระบบ ประกอบด้วย

- ระบบปฏิบัติการ Microsoft Windows 10
- ระบบจัดการฐานข้อมูล MySQL
- โปรแกรมภาษา C#

3.4.2 เครื่องมือที่ใช้ในการรวบรวมข้อมูล ได้แก่ แบบสอบถาม เรื่อง การวิเคราะห์ภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง เป็นแบบสอบถามเชิงคุณภาพสำหรับผู้เชี่ยวชาญ และแบบสอบถามเชิงปริมาณสำหรับผู้ใช้งาน

3.5 การเก็บรวบรวมข้อมูล

การเก็บรวบรวมดำเนินการโดยการจัดทำแบบสอบถาม เรื่อง การวิเคราะห์ภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง ซึ่งได้รับคำแนะนำจากผู้เชี่ยวชาญแล้วจึงปรับปรุงเป็นแบบสอบถามฉบับสมบูรณ์ สำหรับแบบสอบถามเชิงคุณภาพ ได้สัมภาษณ์ผู้เชี่ยวชาญด้านอินเทอร์เน็ตประสานสรรพสิ่ง จำนวน 7 คน นำข้อมูลมาที่ได้มาวิเคราะห์และสรุปประเด็นต่าง ๆ สำหรับแบบสอบถามเชิงปริมาณ ได้ทำการสอบถามกลุ่มตัวอย่างซึ่งเป็นกรณีศึกษาของบุคลากรในกองวิศวกรรมและบริการ การไฟฟ้าส่วนภูมิภาค เขต 1 (ภาคใต้) จังหวัดเพชรบุรี จำนวน 40 คน และนำข้อมูลที่ได้มาทำการวิเคราะห์ ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐาน

จากนั้นจึงนำข้อมูลที่ได้จากแบบสอบถาม มาจำทำกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง

3.6 สถิติที่ใช้ในการวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลการวิจัย ดำเนินการโดยใช้โปรแกรม SPSS (Statistics Package for the Social Sciences) มาวิเคราะห์และประเมินผลจากแบบสอบถามเชิงปริมาณเพื่อหาส่วนเบี่ยงเบนมาตรฐาน (S.D.) และค่าเฉลี่ย ($\overline{X}$) เพื่อใช้ในการวิเคราะห์และรายงานผลค่าทางสถิติ และประมวลผลหาความสัมพันธ์ทางสถิติด้วยระดับความเชื่อมั่น 95 เปอร์เซ็นต์ และมีความคลาดเคลื่อนที่ยอมรับได้ 0.05 เปอร์เซ็นต์ เป็นเกณฑ์ในการยอมรับหรือปฏิเสธสมมุติฐานในการศึกษา

3.7 ระยะเวลาในการดำเนินงาน ดังตัวอย่างในตารางที่ 3.1

ตารางที่ 3.1 ระยะเวลาในการดำเนินงาน

ขั้นตอนการดำเนินงาน	ปีการศึกษา 2560 (กันยายน 2560 – สิงหาคม 2561)					
	ก.ย.-ต.ค.	พ.ย.-ธ.ค.	ม.ค.-ก.พ.	มี.ค.-เม.ย.	พ.ค.-มิ.ย.	ก.ค.-ส.ค.
1. ศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง						
2. ทำจัดทำแบบสอบถามและวิเคราะห์ข้อมูล						
3. วิเคราะห์และออกแบบแอปพลิเคชันระบบประเมินฯ						
4. พัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ						
5. ปรึกษา ขอคำแนะนำจากผู้เชี่ยวชาญ						
6. ปรับปรุง แก้ไข กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ ให้สมบูรณ์						

บทที่ 4
ผลการวิจัย

การศึกษาและวิจัยครั้งนี้เป็นการพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง ซึ่งการวิจัยครั้งนี้มีวัตถุประสงค์ จำนวน 3 ข้อ ดังนี้

1. เพื่อศึกษาและวิเคราะห์ภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง

2. เพื่อพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง

3. เพื่อพัฒนาแอปพลิเคชันระบบประเมินความเสี่ยงด้านภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง

ผู้วิจัยได้ดำเนินการวิจัย โดยเริ่มจากการศึกษาเอกสารและงานวิจัยที่เกี่ยวข้องกับอินเทอร์เน็ตประสานสรรพสิ่ง ความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ เพื่อให้ทราบถึงข้อมูลที่จำเป็นสำหรับการวิจัย ต่อมาจึงทำการวิเคราะห์ความเสี่ยงและภัยคุกคามทางไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง โดยการสัมภาษณ์เชิงลึกผู้เชี่ยวชาญ และใช้แบบสอบถามปลายปิดกับกลุ่มตัวอย่าง ซึ่งเป็นกรณีศึกษาของบุคลากรในกองวิศวกรรมและแผนงานการไฟฟ้าส่วนภูมิภาค เขต 1 (ภาคใต้) จังหวัดเพชรบุรี เพื่อนำข้อมูลที่ได้มาจัดทำกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง โดยอ้างอิงจากจากกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ สหรัฐอเมริกา (National Institute of Standards and Technology: NIST) พร้อมทั้งออกแบบและพัฒนาแอปพลิเคชันระบบประเมินความเสี่ยงด้านภัยคุกคาม และความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง ทำให้ได้มาซึ่งผลการวิจัยดังต่อไปนี้

4.1 ผลการวิจัยตามวัตถุประสงค์ข้อที่ 1

เพื่อศึกษาและวิเคราะห์ภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง โดยได้ทำการวิจัยเชิงคุณภาพและเชิงปริมาณ สำหรับการวิจัยเชิงคุณภาพได้สัมภาษณ์เชิงลึกกลุ่มตัวอย่าง ซึ่งเป็นผู้เชี่ยวชาญด้านอินเทอร์เน็ตประสานสรรพสิ่ง จำนวน 7 คน และสำหรับการวิจัยเชิงคุณภาพได้จัดทำแบบสอบถามกับกลุ่มตัวอย่าง ซึ่งเป็นกรณีศึกษาของบุคลากรในกองวิศวกรรมและแผนงาน การไฟฟ้าส่วนภูมิภาค เขต 1 (ภาคใต้) จังหวัดเพชรบุรี จำนวน 40 คน ลำทำการวิเคราะห์ผลได้ดังต่อไปนี้

4.1.1 ผลการวิจัยเชิงคุณภาพ โดยการวิเคราะห์เนื้อหาจากการสัมภาษณ์เชิงลึกผู้เชี่ยวชาญด้านอินเทอร์เน็ตปรานสรรพสิ่ง จำนวน 7 คน ดังตารางที่ 4.1

ตางรางที่ 4.1 ผลการวิเคราะห์เนื้อหาจากการสัมภาษณ์ผู้เชี่ยวชาญด้านอินเทอร์เน็ตประสานสรรพสิ่ง

ข้อ	คำถาม	ความคิดเห็น
1	ความสำคัญของอินเทอร์เน็ตประสานสรรพสิ่ง	อินเทอร์เน็ตประสานสรรพสิ่งช่วยเพิ่มคุณค่าผลผลิตให้มีคุณภาพ สามารถบูรณาการใช้งานได้ในหลายภาคส่วนของสังคม เช่น สมาร์ทซิตี้ การดูแลสุขภาพของมนุษย์ รวมถึงการคาดการณ์ที่แม่นยำเพื่อนำข้อมูลมาช่วยในการตัดสินใจเชิงธุรกิจ
2	ความเสี่ยงด้านไซเบอร์ ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง	การใช้งานจำเป็นต้องเชื่อมต่ออินเทอร์เน็ตตลอดเวลา และมีอุปกรณ์ที่หลากหลาย จึงมีความเสี่ยงทั้งจากตัวอุปกรณ์และการจัดการระบบ เนื่องจาก อินเทอร์เน็ตประสานสรรพสิ่ง มีคุณสมบัติสามารถใช้งานได้ในหลายสภาพแวดล้อม และทรัพยากรในแต่ละอุปกรณ์ไม่เพียงพอต่อการติดตั้งเทคโนโลยีด้านความปลอดภัย

ตารางที่ 4.1 ผลการวิเคราะห์เนื้อหาจากการสัมภาษณ์ผู้เชี่ยวชาญด้านอินเทอร์เน็ตประสานสรรพสิ่ง (ต่อ)

ข้อ	คำถาม	ความคิดเห็น
3	ภัยคุกคามด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง	ภัยคุกคามด้านไซเบอร์ที่มีผลต่อ อินเทอร์เน็ตประสานสรรพสิ่ง สามารถเกิดได้ในหลากหลายรูปแบบ เนื่องจากในปัจจุบันยังไม่มีการรักษาความมั่นคงปลอดภัยที่ดี เช่น แฮ็กเพื่อขโมยข้อมูลที่เป็นความลับหรือมีความสำคัญ รวมไปถึงภัยคุกคามที่เกิดขึ้นจากคนและอุปกรณ์โดยตรง เช่น การที่ผู้ไม่ประสงค์ดีลักลอบเข้าไปใช้งานหรือทำลายอุปกรณ์ อินเทอร์เน็ตประสานสรรพสิ่ง
4	ความเป็นไปได้ในการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง	ควรทำให้ครอบคลุมทั้งในด้านผู้ใช้งานและผู้พัฒนา ด้านผู้ใช้งานต้องมีความรู้เท่าทันภัยคุกคาม ผู้พัฒนาระบบต้องให้ความสำคัญด้านความปลอดภัย ต้องมีการรักษาความปลอดภัยให้แก่ตัวอุปกรณ์ และซอฟต์แวร์ที่เป็นเทคโนโลยีด้านความปลอดภัย โดยทั้งภาครัฐและภาคเอกชนต้องให้ความร่วมมือกันในการดำเนินการเรื่องนี้
5	การพัฒนาเตรียมบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง	ภาครัฐและภาคเอกชนควรร่วมมือกัน ให้การสนับสนุนบุคลากรที่ทำงานอยู่ในด้าน IT ให้พัฒนาตนเองให้มีความรู้เรื่องความมั่นคงปลอดภัยไซเบอร์เพิ่มมากขึ้น จัดอบรมให้บุคลากรทุกคนมีความรู้ ความเข้าใจ สามารถลดความเสี่ยงจากภัยคุกคามไซเบอร์ได้ สร้างความตระหนักและสร้างกำลังคนด้านความมั่นคงปลอดภัยไซเบอร์
6	ภาพรวมความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง	มีความเสี่ยงมาก เนื่องจากยังอยู่ในขณะเริ่มต้น ยังไม่มีมาตรฐานความปลอดภัยที่ชัดเจน ผู้ผลิตและผู้ใช้งานยังไม่ตระหนักถึงเรื่องความมั่นคงปลอดภัยไซเบอร์เท่าที่ควร อีกทั้งอุปกรณ์มีความหลากหลาย ทำให้ผู้ใช้งานอาจยังไม่คุ้นเคยกับการใช้งานอุปกรณ์แต่ละชนิด

ตารางที่ 4.1 ผลการวิเคราะห์เนื้อหาจากการสัมภาษณ์ผู้เชี่ยวชาญด้านอินเทอร์เน็ตประสานสรรพสิ่ง (ต่อ)

ข้อ	คำถาม	ความคิดเห็น
7	การเตรียมความพร้อมเพื่อรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง	รัฐบาลควรกำหนดมาตรฐานความมั่นคงปลอดภัยที่ชัดเจนและสร้างความรู้ให้ประชาชนทราบถึงวิธีการใช้งานอย่างปลอดภัย หน่วยงานที่ใช้ อินเทอร์เน็ตประสานสรรพสิ่งควรมีการจัดทำกระบวนการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์

แบบสอบถามเชิงปริมาณได้ผลการวิจัย ดังนี้

4.1.2 ผลการวิจัยเชิงปริมาณ โดยการวิเคราะห์และประเมินผลจากแบบสอบถามกับกลุ่มตัวอย่าง ซึ่งเป็นกรณีศึกษาของบุคลากรในกองวิศวกรรมและแผนงาน การไฟฟ้าส่วนภูมิภาค เขต 1 (ภาคใต้) จังหวัดเพชรบุรี จำนวน 40 คน เพื่อหาส่วนเบี่ยงเบนมาตรฐาน (S.D.) และค่าเฉลี่ย ($\overline{X}$) ดังตารางที่ 4.2 และ 4.3

ตารางที่ 4.2 ข้อมูลทั่วไปผู้ตอบแบบสอบถาม

	รายละเอียด	จำนวน	ร้อยละ
	เพศ		
1	**ชาย**	**24**	**60**
2	หญิง	16	40
	อายุ		
1	21 – 30 ปี	5	12.5
2	**31 – 40 ปี**	**20**	**50**
3	41 – 50 ปี	9	22.5
4	51 – 60 ปี	6	15

ตารางที่ 4.2 ข้อมูลทั่วไปผู้ตอบแบบสอบถาม (ต่อ)

	รายละเอียด	จำนวน	ร้อยละ
	ตำแหน่ง		
1	ผู้อำนวยการ	4	10
2	ระดับชำนาญงาน	7	17.5
3	ระดับวิชาการ	8	20
4	**ระดับปฏิบัติงานทั่วไป**	**16**	**40**
5	ระดับลูกจ้าง	2	5
	ระยะเวลที่ปฏิบัติงาน		
1	น้อยกว่า 1 ปี	1	2.5
2	1 – 5 ปี	7	17.5
3	5 – 10 ปี	10	25
4	**มากกว่า 10 ปี**	**22**	**55**
	การประสบภัยคุกคามไซเบอร์		
1	เคย	17	42.5
2	ไม่เคย	22	55

จากตารางที่ 4.2 ข้อมูลของผู้ตอบแบบสอบถาม พบว่า ผู้ตอบแบบสอบถามส่วนใหญ่เป็นเพศชาย จำนวน 24 คน (ร้อยละ 60) มีอายุระหว่าง 31 – 41 ปี จำนวน 20 คน (ร้อยละ 50) มีตำแหน่งอยู่ในระดับปฏิบัติงานทั่วไป จำนวน 16 คน (ร้อยละ 40) มีระยะเวลาที่ปฏิบัติงานมากกว่า 10 ปี จำนวน 22 คน (ร้อยละ 55) และไม่เคยประสบภัยคุกคามไซเบอร์ จำนวน 22 คน (ร้อยละ 55)

ตารางที่ 4.3 ความคิดเห็นเกี่ยวกับความเสี่ยงของภัยคุกคามทางไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง

ข้อคำถาม	$\bar{X}$	S.D.	แปลผล
1. การกำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์	3.50	1.10	มาก
2. การปกป้องดูแลด้านความมั่นคงปลอดภัยไซเบอร์	3.39	1.24	ปานกลาง
3. การตรวจพบเหตุภัยคุกคามไซเบอร์	3.11	1.20	ปานกลาง
4. การรับมือภัยคุกคามไซเบอร์	3.18	1.22	ปานกลาง
5. การกู้คืนข้อมูลหลังเหตุภัยคุกคามไซเบอร์	3.30	1.12	ปานกลาง
ระดับความคิดเห็นเฉลี่ย	**3.30**	**1.18**	**ปานกลาง**

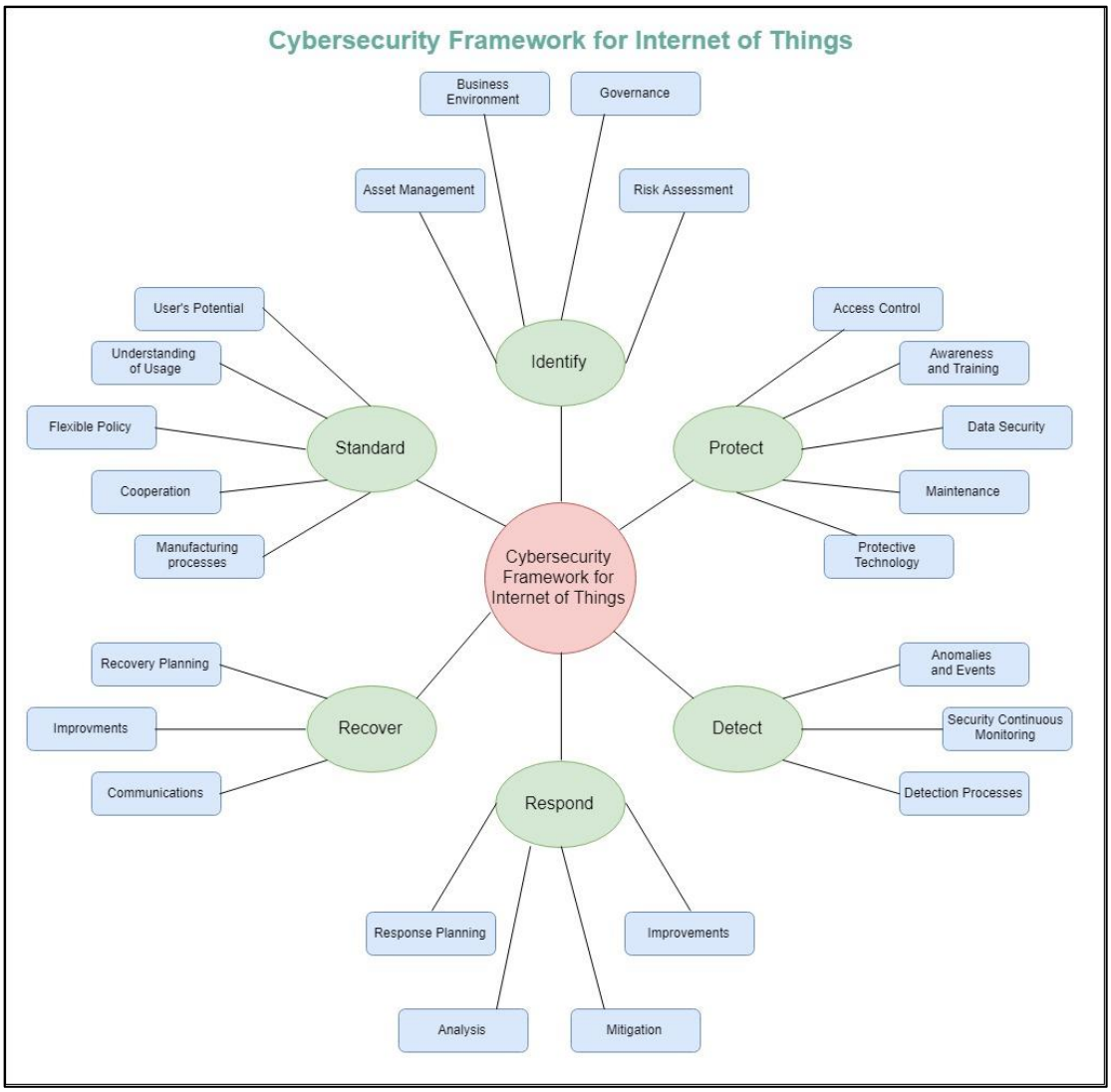
จากตารางที่ 4.3 ได้สรุปความคิดเห็นเกี่ยวกับความเสี่ยงของภัยคุกคามทางไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง จำนวน 40 ชุด พบว่า มีความเสี่ยงอยู่ในระดับปานกลาง ($\bar{X}$ = 3.30)

เมื่อพิจารณาเป็นรายข้อ พบว่า ด้านการกำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์ มีความเสี่ยงอยู่ในระดับมาก ($\bar{X}$ = 3.50) ด้านการปกป้องดูแลด้านความมั่นคงปลอดภัยไซเบอร์ มีความเสี่ยงอยู่ในระดับปานกลาง ($\bar{X}$ = 3.39) ด้านการตรวจพบเหตุภัยคุกคามไซเบอร์ มีความเสี่ยงอยู่ในระดับปานกลาง ($\bar{X}$ = 3.11) ด้านการรับมือภัยคุกคามทางไซเบอร์ มีความเสี่ยงอยู่ในระดับปานกลาง ($\bar{X}$ = 3.18) และความคิดเห็นด้านการกู้คืนข้อมูลหลังเหตุภัยคุกคามไซเบอร์ มีความเสี่ยงอยู่ในระดับปานกลาง ($\bar{X}$ = 3.30)

4.2 ผลการวิจัยตามวัตถุประสงค์ข้อที่ 2

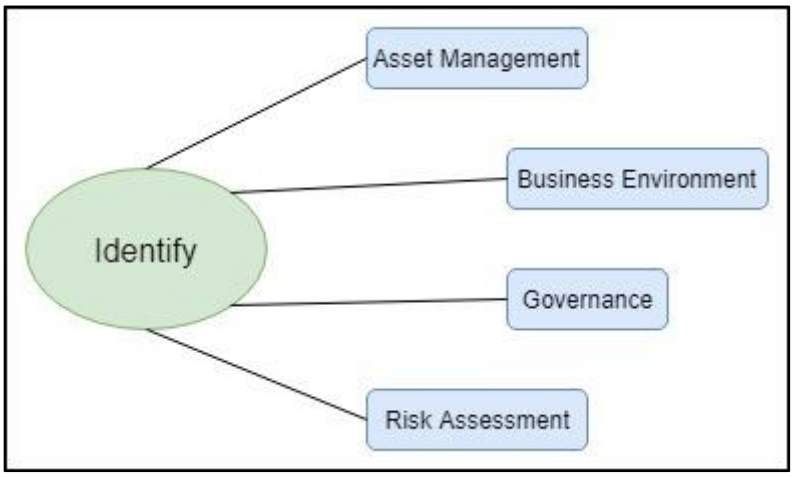
จากวัตถุประสงค์ข้อที่ 2 เพื่อพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง ผู้วิจัยได้จัดทำกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง โดยใช้ข้อมูลจากการวิเคราะห์แบบสอบถามเพื่อการวิเคราะห์ความเสี่ยงของภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง และอ้างอิงจากกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ สหรัฐอเมริกา (National Institute of Standards and Technology: NIST) ซึ่งประกอบไปด้วย 6 ฟังก์ชันหลัก รวมทั้งฟังก์ชันย่อย ดังภาพประกอบที่ 4.1

1. การกำหนดมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ (Identify)
2. การปกป้องดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (Protect)
3. การตรวจจับเหตุการ์ภัยคุกคามทางไซเบอร์ (Detect)
4. การรับมือภัยคุกคามทางไซเบอร์ (Respond)
5. การกู้คืน (Recover)
6. การกำหนดมาตรฐาน (Standard)



ภาพประกอบที่ 4.1 กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง

4.2.1 การกำหนดมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ (Identify) ประกอบด้วย การจัดการสินทรัพย์ (Asset Management), สภาพแวดล้อมทางธุรกิจ (Business Environment), การกำกับดูแล (Governance) และการประเมินความเสี่ยง (Risk Assessment) ดังภาพประกอบที่ 4.2



ภาพประกอบที่ 4.2 การกำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์ (Identify)

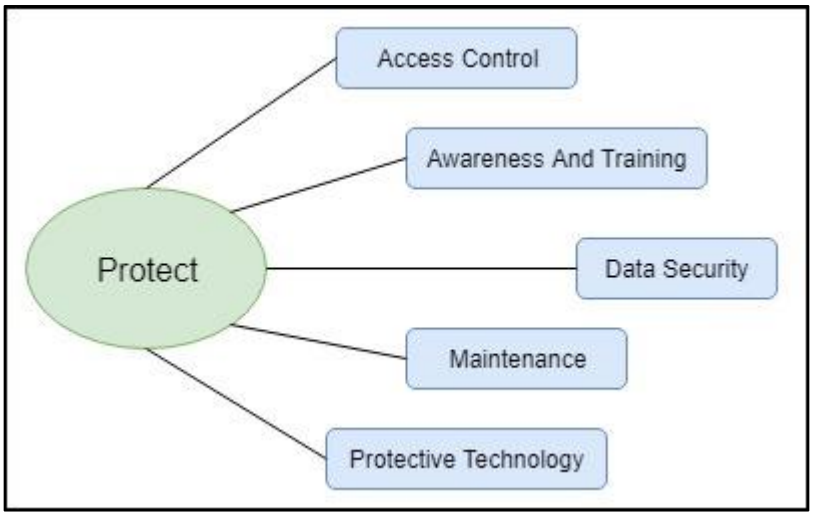
4.2.1.1 การจัดการสินทรัพย์ (Asset Management) มีคลังจัดเก็บอุปกรณ์อินเทอร์เน็ตประสานสรรพสิ่ง อย่างเป็นระบบ สามารถสืบค้นได้ และจัดลำดับความสำคัญของแต่ละอุปกรณ์

4.2.1.2 สภาพแวดล้อมทางธุรกิจ (Business Environment) มีการกำหนดวัตถุประสงค์ในการใช้งานอุปกรณ์ อินเทอร์เน็ตประสานสรรพสิ่ง ตามบริบทของอุปกรณ์ โดยกำหนดขอบเขตการใช้งานเพื่อให้บรรลุวัตถุประสงค์ของการดำเนินงาน

4.2.1.3 การกำกับดูแล (Governance) มีการควบคุมดูแลด้านกฎหมาย การจัดการสภาพแวดล้อมการใช้งาน และกฎ ระเบียบการใช้งานอุปกรณ์ อินเทอร์เน็ตประสานสรรพสิ่ง

4.2.1.4 การประเมินความเสี่ยง (Risk Assessment) การรับทราบถึงช่องโหว่และความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีผลต่ออุปกรณ์ อินเทอร์เน็ตประสานสรรพสิ่ง นำมาจัดลำดับความสำคัญ และบันทึกไว้เป็นลายลักษณ์อักษร

4.2.2 การปกป้องดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (Protect) ประกอบด้วย ควบคุมการเข้าถึง (Access Control), การสร้างความตระหนักและฝึกอบรม (Awareness and Training), การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security), การซ่อมบำรุง (Maintenance) และเทคโนโลยีการป้องกัน (Protective Technology) ดังภาพประกอบที่ 4.3



ภาพประกอบที่ 4.3 การปกป้องดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (Protect)

4.2.2.1 ควบคุมการเข้าถึง (Access Control) มีการควบคุมการเข้าถึงและใช้งานอุปกรณ์ อินเทอร์เน็ตประสานสรรพสิ่ง โดยการตรวจสอบสิทธิ์จากข้อมูลประจำตัว และมีการรักษาความปลอดภัยในการควบคุมการเข้า-ออกอาคาร

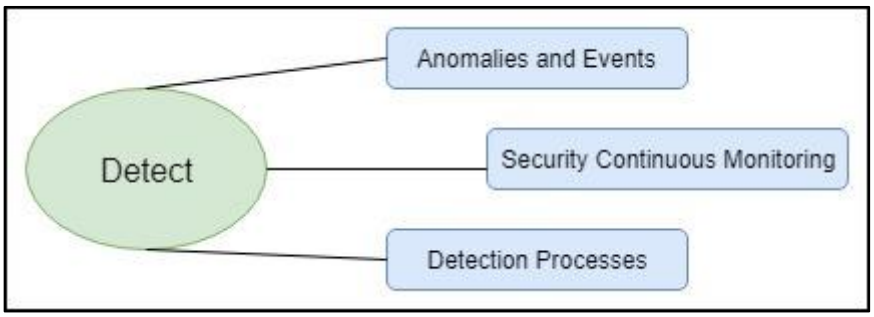
4.2.2.2 การสร้างความตระหนักและฝึกอบรม (Awareness and Training) มีการสร้างความตระหนักให้แก่บุคลากรผู้เกี่ยวข้องทราบและเข้าใจถึงบทบาทความรับผิดชอบของตนเอง และมีการฝึกอบรมการใช้งานอุปกรณ์ อินเทอร์เน็ตประสานสรรพสิ่ง ให้แก่ผู้ใช้งานทุกคน

4.2.2.3 การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security) ข้อมูลทั้งหมดต้องได้รับการปกป้อง ไม่ให้รั่วไหล ทั้งที่อยู่ระหว่างการใช้งาน หรือที่อยู่ในอุปกรณ์ที่ยกเลิกการใช้งานแล้ว

4.2.2.4 การซ่อมบำรุง (Maintenance) มีกำหนดการซ่อมบำรุงอุปกรณ์อินเทอร์เน็ตประสานสรรพสิ่ง อย่างเป็นขั้นตอน ด้วยเครื่องมือที่ได้รับการอนุมัติและควบคุม

4.2.2.5 เทคโนโลยีการป้องกัน (Protective Technology) มีการติดตั้งเทคโนโลยีด้านความมั่นคงปลอดภัยในอุปกรณ์ อินเทอร์เน็ตประสานสรรพสิ่ง ที่ทันสมัยและได้รับการอัพเดทสม่ำเสมอ

4.2.3 การตรวจจับเหตุการ์ภัยคุกคามทางไซเบอร์ (Detect) ประกอบด้วย เหตุการณ์และความผิดปกติ (Anomalies and Events), การเฝ้าระวังด้านความมั่นคงปลอดภัยอย่างต่อเนื่อง (Security Continuous Monitoring) และกระบวนการตรวจจับ (Detection Processes) ดังภาพประกอบที่ 4.4



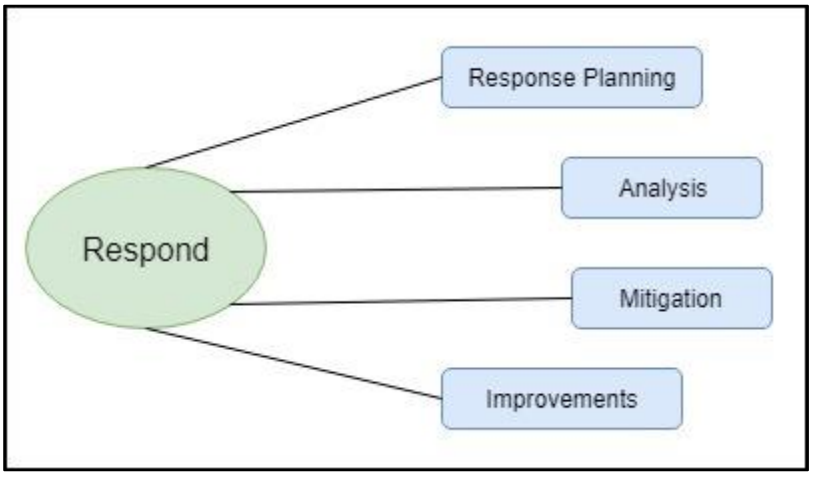
ภาพประกอบที่ 4.4 การตรวจจับเหตุการณ์ภัยคุกคามทางไซเบอร์ (Detect)

4.2.3.1 เหตุการณ์และความผิดปกติ (Anomalies and Events) มีการตรวจหาเหตุการณ์ผิดปกติสำหรับการใช้งานอุปกรณ์ อินเทอร์เน็ตประสานสรรพสิ่ง โดยนำเหตุการณ์ที่ตรวจพบมาวิเคราะห์และแจ้งเตือน

4.2.3.2 การเฝ้าระวังด้านความมั่นคงปลอดภัยอย่างต่อเนื่อง (Security Continuous Monitoring) มีการเฝ้าระวังทั้งทางเครือข่าย ตัวอุปกรณ์ และผู้คน รวมไปถึงการตรวจหาช่องโหว่ด้วย

4.2.3.3 กระบวนการตรวจจับ (Detection Processes) มีการกำหนดบทบาทและความรับผิดชอบในการตรวจหาเหตุการณ์ผิดปกติสำหรับการใช้งานอุปกรณ์ อินเทอร์เน็ตประสานสรรพสิ่ง โดยต้องมีการทดสอบ และปรับปรุงอย่างต่อเนื่อง

4.2.4 การรับมือภัยคุกคามทางไซเบอร์ (Respond) ประกอบด้วย วางแผนการรับมือ (Response Planning), การสื่อสาร (Communications), การวิเคราะห์ (Analysis), การบรรเทาความเสียหาย (Mitigation) และการปรับปรุง (Improvements) ดังภาพประกอบที่ 4.5



ภาพประกอบที่ 4.5 การรับมือภัยคุกคามทางไซเบอร์ (Respond)

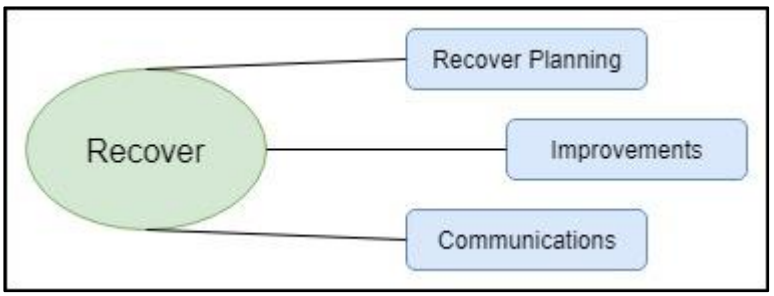
4.2.4.1 วางแผนการรับมือ (Response Planning) มีการวางแผนรับมือเหตุภัยคุกคามทางไซเบอร์ในระหว่างและหลังการโจมตีอุปกรณ์ อินเทอร์เน็ตประสานสรรพสิ่ง

4.2.4.2 การวิเคราะห์ (Analysis) มีการวิเคราะห์เพื่อทราบถึงผลกระทบที่จะเกิดจากเหตุภัยคุกคามทางไซเบอร์สำหรับอุปกรณ์ อินเทอร์เน็ตประสานสรรพสิ่ง นำไปจัดทำแผนรับมือและประกาศให้ผู้เกี่ยวข้องทราบ

4.2.4.3 การบรรเทาความเสียหาย (Mitigation) มีกระบวนการบรรเทาความเสียหายจากเหตุการณ์ที่เคยเกิดขึ้น และหากค้นพบช่องโหว่ใหม่ก็ต้องหาวิธีบรรเทาความเสียหายด้วย

4.2.4.4 การปรับปรุง (Improvements) มีการเรียนรู้จากเหตุการณ์ภัยคุกคามไซเบอร์ที่มีผลต่ออุปกรณ์ อินเทอร์เน็ตประสานสรรพสิ่ง ที่ผ่านมา รวบรวมข้อมูล และนำมาพัฒนากลยุทธ์การรับมือต่อไป

4.2.5 การกู้คืน (Recover) ประกอบด้วย วางแผนการรับมือ (Recover Planning), การปรับปรุง (Improvements) และการสื่อสาร (Communications) ดังภาพประกอบที่ 4.6



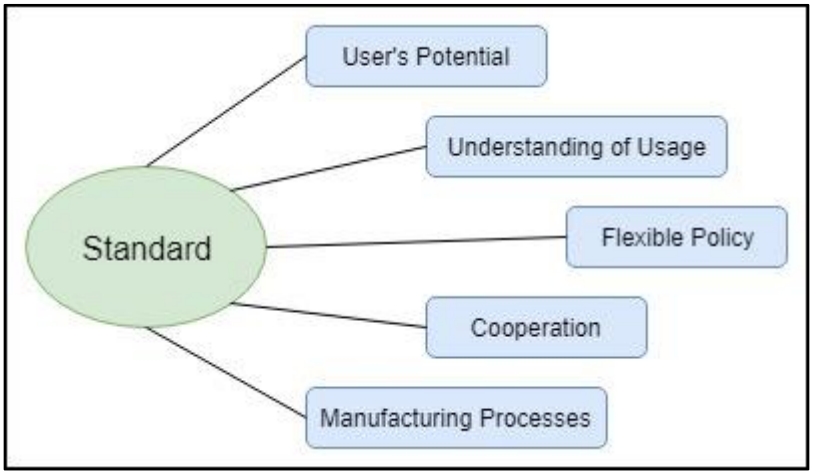
ภาพประกอบที่ 4.6 การกู้คืน (Recover)

4.2.5.1 วางแผนการกู้คืน (Recover Planning) มีการวางแผนการกู้คืนสภาพการใช้งานเหตุภัยคุกคามทางไซเบอร์ในระหว่างและหลังการโจมตีอุปกรณ์ อินเทอร์เน็ตประสานสรรพสิ่ง

4.2.5.2 การปรับปรุง (Improvements) มีการปรับปรุงการวางแผนและกระบวนการกู้คืน โดยรวบรวมข้อมูลจากเหตุภัยคุกคามไซเบอร์ในอุปกรณ์ อินเทอร์เน็ตประสานสรรพสิ่ง ที่ผ่านมา เพื่อกำหนดกลยุทธ์ให้ทันสมัย

4.2.5.3 การสื่อสาร (Communications) มีการประชาสัมพันธ์และประสานงานกับหน่วยงานที่เกี่ยวข้อง ทั้งภายในและภายนอกเพื่อให้ทราบเมื่อมีกิจกรรมการกู้คืนอุปกรณ์อินเทอร์เน็ตประสานสรรพสิ่ง

4.2.6 การกำหนดมาตรฐาน (Standard) ประกอบด้วย ศักยภาพของผู้ใช้ (User's Potential), ความเข้าใจในการใช้งาน (Understanding of Usage), นโยบายที่ยืดหยุ่น (Flexible Policy), ความร่วมมือ (Cooperation) และกระบวนการผลิต (Manufacturing Processes) ดังภาพประกอบที่ 4.7



ภาพประกอบที่ 4.7 การกำหนดมาตรฐาน (Standard)

4.2.6.1 ศักยภาพของผู้ใช้ (User's Potential) มีการกำหนดทักษะ ความเข้าใจในการใช้งานอุปกรณ์ อินเทอร์เน็ตประสานสรรพสิ่ง ของผู้ใช้แต่ละคน ด้านการรักษาความมั่นคงปลอดภัยและภัยคุกคามทางไซเบอร์ รวมถึงการแก้ปัญหาเมื่อเกิดเหตุการณ์ภัยคุกคาม

4.2.6.2 ความเข้าใจในการใช้งาน (Understanding of Usage) การใช้งานอุปกรณ์อินเทอร์เน็ตประสานสรรพสิ่ง ต้องใช้งานตามวัตถุประสงค์ของอุปกรณ์นั้น ทั้งด้านการเชื่อมต่อสถานที่ใช้งาน และมีการประกาศวิธีใช้งานและผู้รับผิดชอบอย่างชัดเจน

4.2.6.3 นโยบายที่ยืดหยุ่น (Flexible Policy) การกำหนดนโยบายสำหรับการใช้งาน อุปกรณ์ อินเทอร์เน็ตประสานสรรพสิ่ง ต้องคำนึงถึงความแตกต่างกันของวิธีการใช้งานของแต่ละอุปกรณ์ และเทคโนโลยีที่เปลี่ยนแปลงในอนาคต

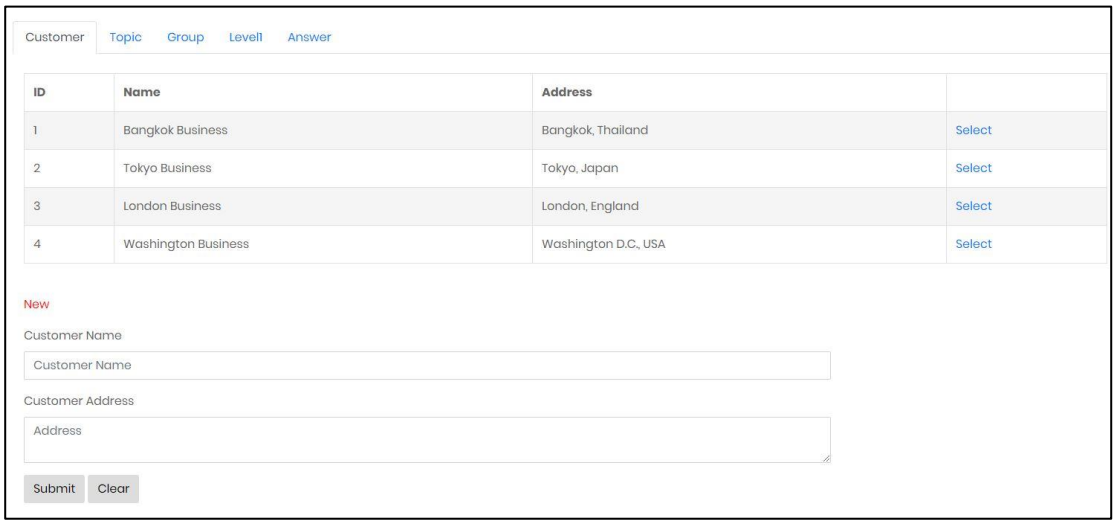
4.2.6.4 ความร่วมมือ (Cooperation) มีการให้ความร่วมมือ ทั้งกับหน่วยงานภายในและภายนอกในเรื่องของการแบ่งปันข้อมูล วิธีปฏิบัติ กระบวนการรักษาความมั่นคงปลอดภัยไซเบอร์ และประสบการณ์ของแต่ละองค์กร

4.2.6.5 กระบวนการผลิต (Manufacturing Processes) มีการกำหนดคุณภาพวัตถุดิบที่นำมาใช้ในการผลิตอุปกรณ์ การติดตั้งทรัพยากรและเทคโนโลยีด้านความมั่นคงปลอดภัย โดยผู้ผลิตและผู้พัฒนาต้องคำนึงเรื่องความมั่นคงปลอดภัยเป็นหลัก

4.3 ผลการวิจัยตามวัตถุประสงค์ข้อที่ 3

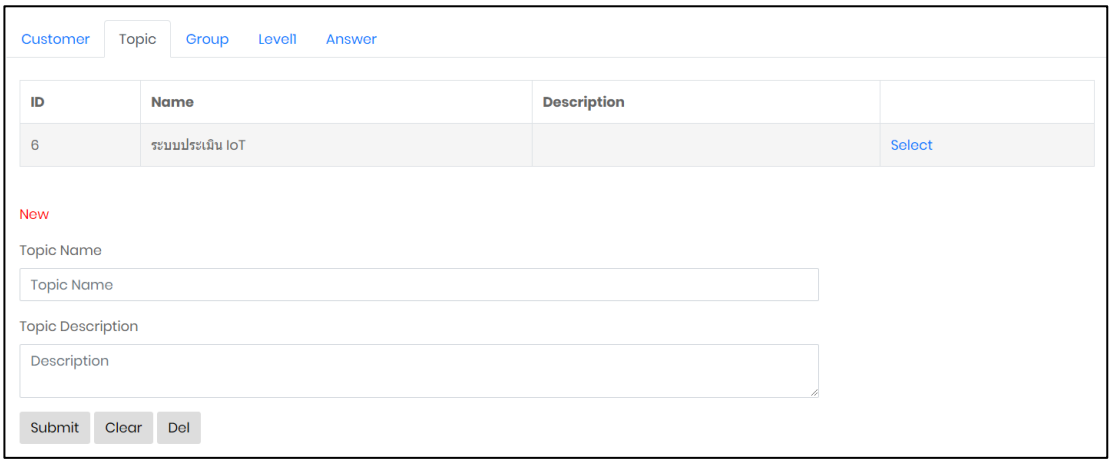
จากวัตถุประสงค์ข้อที่ 3 เพื่อพัฒนาแอปพลิเคชันระบบประเมินความเสี่ยงด้านภัยคุกคามและความเสี่ยงด้านไซเบอร์ ซึ่งจะทำให้องค์กรสามารถเตรียมความพร้อมและปรับปรุงนโยบายด้านความมั่นคงปลอดภัยไซเบอร์สำหรับการใช้อินเทอร์เน็ตประสานสรรพสิ่งในองค์กรได้ ดังนี้

4.3.1 หน้าจอบันทึกข้อมูลองค์กรที่ทำการประเมิน โดยทำการบันทึกชื่อและที่อยู่องค์กรที่จะทำการประเมิน ดังภาพประกอบที่ 4.8



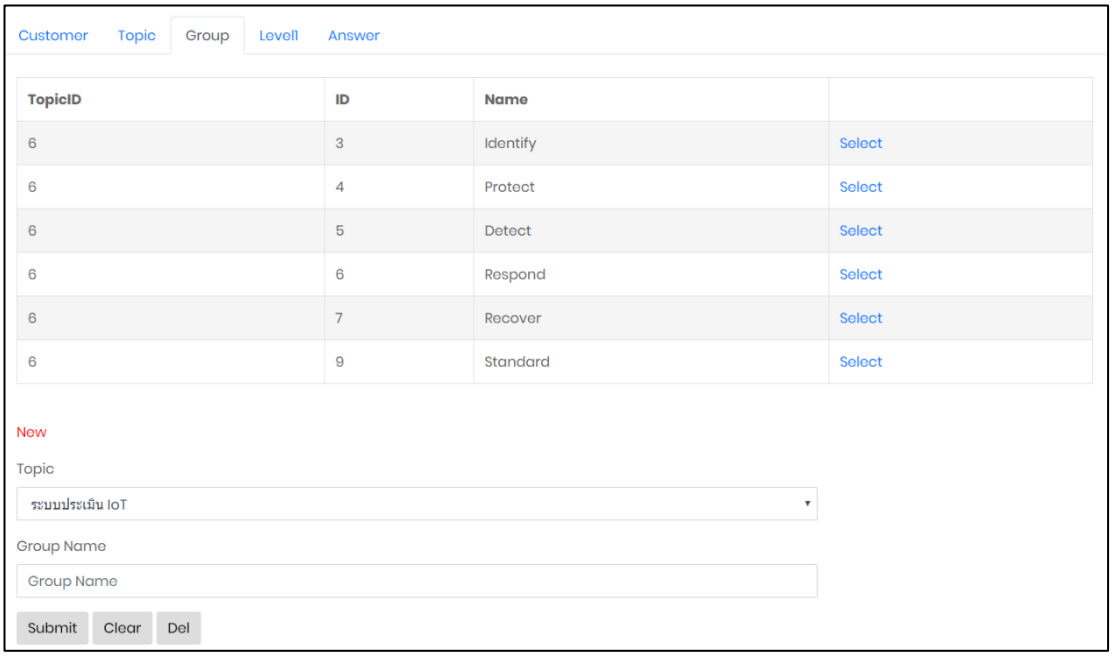
ภาพประกอบที่ 4.8 หน้าจอบันทึกข้อมูลองค์กรที่ทำการประเมิน

4.3.2 หน้าจอบันทึกชื่อการประเมิน โดยทำการบันทึกชื่อสำหรับการประเมินในแต่ละองค์กร ดังภาพประกอบที่ 4.9



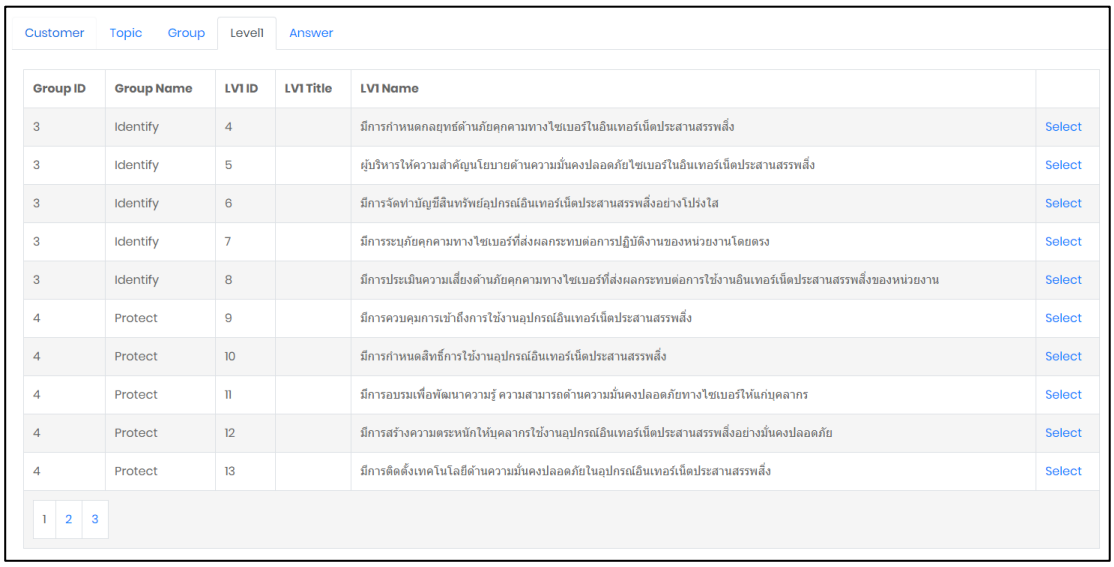
ภาพประกอบที่ 4.9 หน้าจอบันทึกชื่อการประเมิน

4.3.3 หน้าจอบันทึกหัวข้อหลักสำหรับการประเมิน โดยทำการบันทึกชื่อหัวข้อหลักสำหรับการประเมิน ดังภาพประกอบที่ 4.10



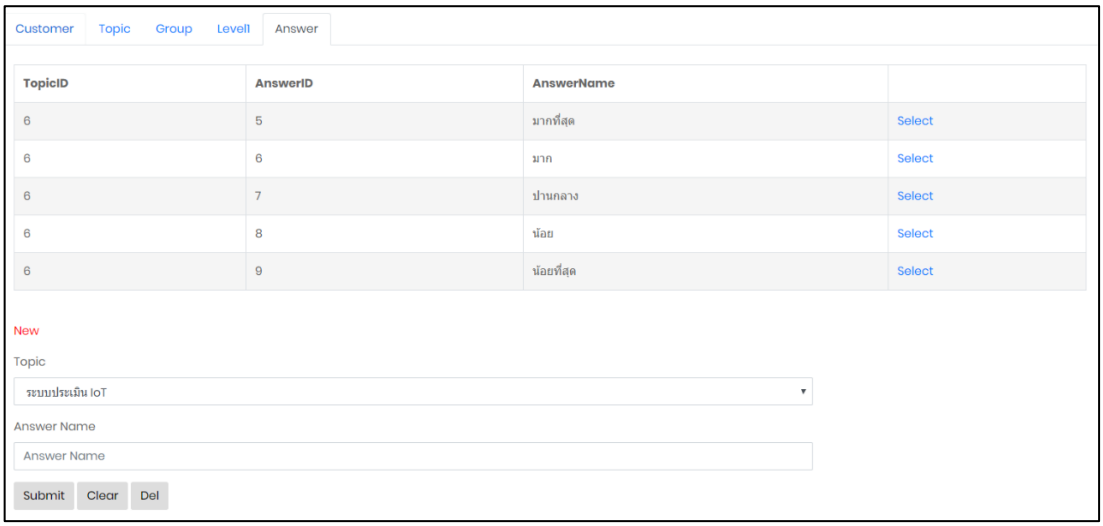
ภาพประกอบที่ 4.10 หน้าจอบันทึกหัวข้อหลักสำหรับการประเมิน

4.3.4 หน้าจอบันทึกหัวข้อย่อยสำหรับการประเมิน โดยทำการบันทึกหัวข้อย่อยสำหรับการประเมิน ดังภาพประกอบที่ 4.11



ภาพประกอบที่ 4.11 หน้าจอบันทึกหัวข้อย่อยสำหรับการประเมิน

4.3.5 หน้าจอสำหรับบันทึกตัวเลือกคำตอบสำหรับการประเมิน โดยทำการบักทึกตัวเลือกคำตอบสำหรับการประเมิน ดังภาพประกอบที่ 4.12

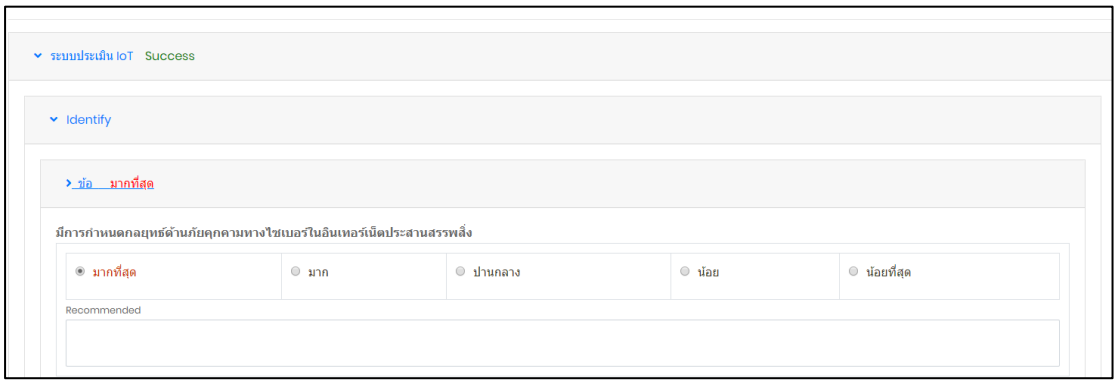


ภาพประกอบที่ 4.12 หน้าจอสำหรับบันทึกตัวเลือกคำตอบสำหรับการประเมิน

4.3.6 หน้าจอสำหรับเลือกข้อมูลองค์กรที่จะทำการประเมิน โดยทำการเลือกชื่อองค์กรที่จะประเมินในแต่ละครั้ง ดังภพประกอบที่ 4.13

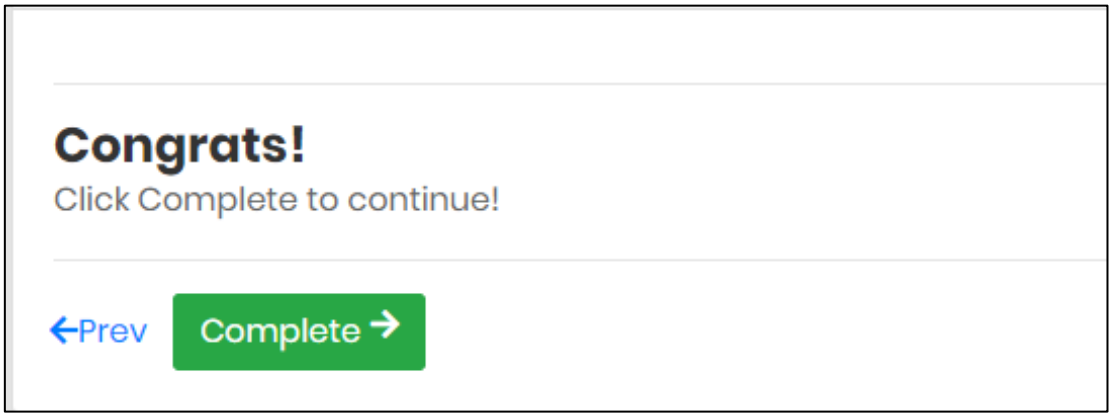
ภาพประกอบที่ 4.13 หน้าจอสำหรับเลือกข้อมูลองค์กรที่จะทำการประเมิน

4.3.7 หน้าจอสำหรับทำการประเมิน โดยผู้ประเมินในแต่ละองค์กรจะทำการประเมินตามหัวข้อและตัวเลือกคำตอบที่ได้กำหนดไว้ ดังภาพประกอบที่ 4.14



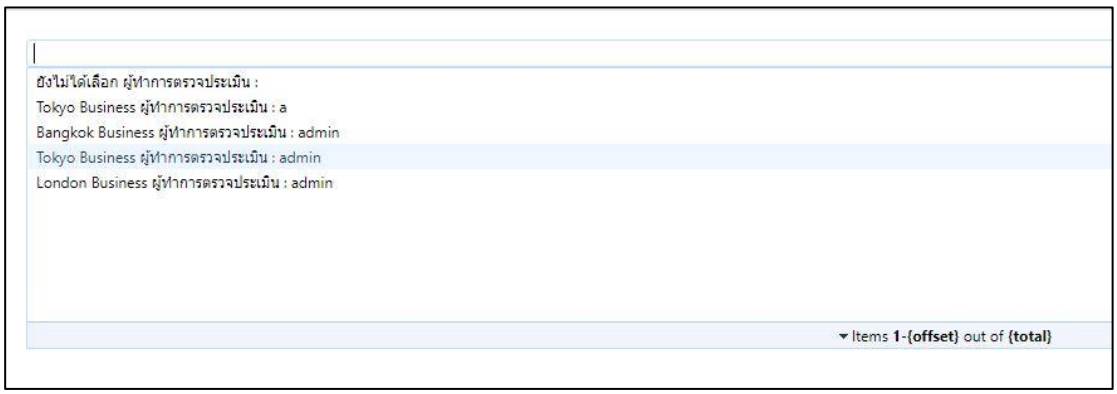
ภาพประกอบที่ 4.14 หน้าจอสำหรับทำการประเมิน

4.3.8 หน้าจอสำหรับส่งผลการประเมิน โดยเมื่อทำการประเมินครบทุกหัวข้อแล้วจึงกด Complete เพื่อบันทึกผลการประเมิน หรือกด Previous เพื่อกลับไปแก้ไขการประเมิน ดังภาพประกอบที่ 4.15



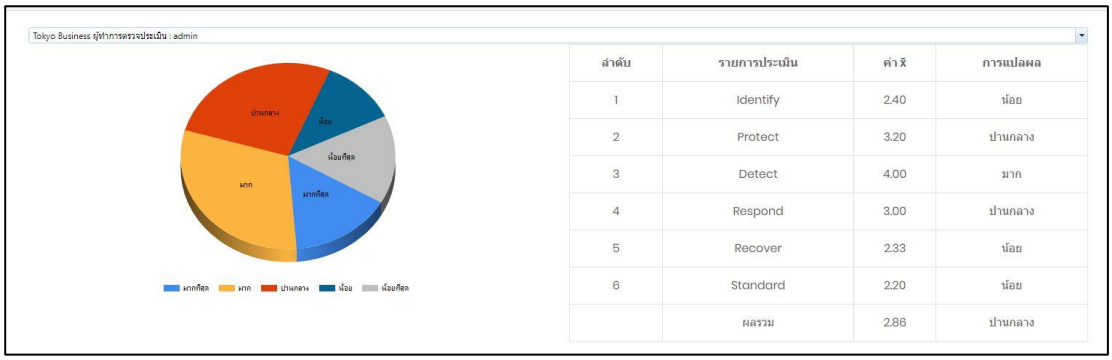
ภาพประกอบที่ 4.15 หน้าจอสำหรับส่งผลการประเมิน

4.3.9 หน้าจอสำหรับเลือกดูรายงานการประเมิน โดยทำการเลือกชื่อองค์กรที่ได้ทำการประเมินสำเร็จแล้ว เพื่อดูสรุปผลการประเมิน ดังภพประกอบที่ 4.16



ภาพประกอบที่ 4.16 หน้าจอสำหรับเลือกดูรายงานการประเมิน

4.3.10 หน้าจอรายงานการผลประเมิน โดยหลังจากที่เลือกชื่อองค์กรที่ได้ทำการประเมินสำเร็จแล้ว ระบบจะแสดงสรุปผลการประเมินของแต่ละองค์กร ดังภาพประกอบที่ 4.17



ลำดับ	รายการประเมิน	ค่า ร้	การแปลผล
1	Identify	2.40	น้อย
2	Protect	3.20	ปานกลาง
3	Detect	4.00	มาก
4	Respond	3.00	ปานกลาง
5	Recover	2.33	น้อย
6	Standard	2.20	น้อย
	ผลรวม	2.86	ปานกลาง

ภาพประกอบที่ 4.17 หน้าจอรายงานการผลประเมิน

บทที่ 5
สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

การศึกษาและวิจัยนี้ เป็นการพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง เป็นการวิจัยเพื่อ 1) เพื่อศึกษาและวิเคราะห์ภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง 2) เพื่อพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง และ 3) เพื่อพัฒนาแอปพลิเคชันระบบประเมินความเสี่ยงด้านภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง นำเสนอตามลำดับต่อไปนี้

5.1 สรุปผลการวิจัย

1. ศึกษาและวิเคราะห์ภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง ดำเนินการวิจัยทั้งเชิงคุณภาพและเชิงปริมาณ โดยใช้การสัมภาษณ์เชิงลึกผู้เชี่ยวชาญด้านอินเทอร์เน็ตประสานสรรพสิ่ง จำนวน 7 คน และแบบสอบถามปลายปิดกับกลุ่มตัวอย่างซึ่งเป็นกรณีศึกษาของบุคลากรในกองวิศวกรรมและแผนงาน การไฟฟ้าส่วนภูมิภาค เขต 1 (ภาคใต้) จังหวัดเพชรบุรี จำนวน 40 คน สรุปผลการวิจัยได้ดังนี้

1.1 สรุปผลการวิจัยเชิงคุณภาพ โดยผู้เชี่ยวชาญทุกท่านมีความเห็นตรงกันว่าอินเทอร์เน็ตประสานสรรพสิ่งมีบทบาทและความสำคัญแก่สังคมในยุคปัจจุบัน มีความเสี่ยงจากภัยคุกคามทางไซเบอร์มาก เนื่องจากยังไม่มีมาตรฐานการรักษาความมั่นคงปลอดภัยที่เหมาะสมโดยเฉพาะ การใช้งานที่ต้องเชื่อมต่อกับเครือข่ายและอุปกรณ์อื่น และผู้ใช้งานยังไม่คุ้นชินกับการใช้งานอุปกรณ์ชนิดใหม่ ๆ อีกทั้งอุปกรณ์บางชนิดก็ไม่ได้ถูกออกแบบมาเพื่อเชื่อมต่อกับเครือข่าย ดังนั้นการรักษาความมั่นคงปลอดภัยจึงควรกำหนดมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง การใช้งานควรตระหนักถึงการรักษาความมั่นคงปลอดภัยเป็นเรื่องสำคัญ และสร้างความทักษะด้านความมั่นคงปลอดภัยให้แก่ผู้ใช้และผู้พัฒนาเป็นเรื่องสำคัญ

1.2 สรุปผลการวิจัยเชิงปริมาณ โดยกลุ่มตัวอย่างซึ่งเป็นกรณีศึกษาของบุคลากรในกองวิศวกรรมและแผนงาน การไฟฟ้าส่วนภูมิภาค เขต 1 (ภาคใต้) จังหวัดเพชรบุรี จำนวน 40 คน มีความคิดเห็นเกี่ยวกับความเสี่ยงของภัยคุกคามทางไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง แยกเป็นรายข้อได้ดังนี้ ด้านการกำหนดมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ มีความเสี่ยงอยู่ในระดับมาก ($\overline{X}$ = 3.50) ด้านการปกป้องดูแลด้านความมั่นคงปลอดภัยไซเบอร์ มีความเสี่ยงอยู่ในระดับปานกลาง ($\overline{X}$ = 3.39) ด้านการตรวจพบเหตุภัยคุกคามไซเบอร์ มีความเสี่ยงอยู่ในระดับปานกลาง ($\overline{X}$ = 3.11) ด้านการรับมือภัยคุกคามไซเบอร์ มีความเสี่ยงอยู่ในระดับปานกลาง ($\overline{X}$ = 3.18) ด้านการกู้คืนข้อมูลหลังเหตุภัยคุกคามไซเบอร์ มีความเสี่ยงอยู่ในระดับปานกลาง ($\overline{X}$ = 3.30) และระดับความคิดเห็นเฉลี่ยจากทุกหัวข้อดังกล่าว มีความเสี่ยงอยู่ในระดับปานกลาง ($\overline{X}$ = 3.30)

2. พัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง

2.1 จากผลการศึกษาและวิเคราะห์ภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง ทำให้ได้ทราบถึงภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีอยู่และที่อาจเกิดขึ้นได้

2.2 จัดทำกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง โดยใช้ข้อมูลจากการวิเคราะห์แบบสอบถามเพื่อการวิเคราะห์ความเสี่ยงของภัยคุกคามทาง ไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง และอ้างอิงจากกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ สหรัฐอเมริกา (National Institute of Standards and Technology: NIST) ทำให้ได้มาซึ่งฟังก์ชัน ทั้ง 6 ด้าน ดังนี้ 1) การกำหนดมาตรการด้านความมั่นคงปลอดภัย (Identify) 2) การปกป้องดูแลด้านความมั่นคงปลอดภัย (Protect) 3) การตรวจจับเหตุการ์ภัยคุกคามทางไซเบอร์ (Detect) 4) การรับมือภัยคุกคามทางไซเบอร์ (Respond) 5) การกู้คืน (Recover) 6) การกำหนดมาตรฐาน (Standard)

3. พัฒนาแอปพลิเคชันระบบประเมินความเสี่ยงด้านภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง

เมื่อได้กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่งซึ่งทำให้ทราบถึงกรอบวิธีปฏิบัติและแนวทางในการใช้งานอย่างมั่นคงปลอดภัยแล้ว จึงจัดทำแอปพลิเคชันระบบประเมิน ด้วยการนำฟังก์ชันทั้ง 6 ด้านใช้สำหรับการประเมินความเสี่ยง

ด้านภัยคุกคามทางไซเบอร์ในองค์กร เพื่อให้ได้แนวทางและเตรียมการป้องกันความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง

5.2 อภิปรายผล

การวิเคราะห์ความเสี่ยงด้านภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง พบว่ามีความเสี่ยงมาก และการรักษาความมั่นคงปลอดภัยของหน่วยงานที่ใช้อินเทอร์เน็ตประสานสรรพสิ่งมีความเสี่ยงอยู่ในระดับปานกลาง จากข้อมูลที่ได้นำมาพัฒนากรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง ประกอบด้วยฟังก์ชันหลัก 6 ด้าน 1) การกำหนดมาตรการด้านความมั่นคงปลอดภัย (Identify) 2) การปกป้องดูแลด้านความมั่นคงปลอดภัย (Protect) 3) การตรวจจับเหตุการ์ภัยคุกคามทางไซเบอร์ (Detect) 4) การรับมือภัยคุกคามทางไซเบอร์ (Respond) 5) การกู้คืน (Recover) 6) การกำหนดมาตรฐาน (Standard) และฟังก์ชันย่อย สำหรับใช้ในการประเมินความเสี่ยงด้านไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่งในองค์กรโดยใช้แอปพลิเคชันระบบประเมินความเสี่ยงด้านภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง เพื่อให้บุคลากรขององค์กรนั้น ประเมินถึงมาตรการรักษาความมั่นคงปลอดภัย ไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่งที่ใช้อยู่ในองค์กรมีความเหมาะสมหรือมีความเสี่ยงมากน้อยเพียงใด และนำผลการประเมินที่ได้มาเป็นข้อปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยขององค์กรต่อไป

ทั้งนี้ ผลการวิจัยได้สอดคล้องกับงานวิจัยของ สรวิศ บุญมี ที่ได้ศึกษาเรื่องความมั่นคงปลอดภัยของ IoT โดยสรุปว่าผู้ที่เกี่ยวข้อง ควรให้ความสำคัญด้านความมั่นคงปลอดภัย ตั้งแต่ขั้นตอนการออกแบบและการพัฒนาเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นอย่างมากในภายหลัง

5.3 ปัญหาและอุปสรรค

5.3.1 การศึกษาเอกสารที่เกี่ยวข้องกับงานวิจัยจำนวนมาก ทำให้ได้ความรู้ ความเข้าใจ และทราบถึงประเด็นปัญหาสำหรับหัวข้องานวิจัยที่แท้จริง หากศึกษาเอกสารที่เกี่ยวข้องน้อย อาจส่งผลต่อความเข้าใจในงานของตนเอง

5.3.2 ผู้วิจัยจำเป็นต้องใช้เวลากับงานวิจัยมากเพื่อให้งานสำเร็จลุล่วง หากมีกิจกรรมอื่นเข้ามาแทรกอาจส่งผลให้ทำงานวิจัยไม่สำเร็จ จึงต้องบริหารเวลาทำงานวิจัยและกิจกรรมต่าง ๆ ให้ดี

5.3.3 การพัฒนาแอปพลิเคชันระบบประเมินความเสี่ยงด้านภัยคุกคามและความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง จำเป็นต้องมีความเชี่ยวชาญด้านการเขียนโปรแกรม ผู้วิจัยควรศึกษาด้านการเขียนโปรแกรมเพิ่มเติม และขอคำปรึกษาจากผู้เชี่ยวชาญโดยตรง

5.4 ข้อเสนอแนะ

5.4.1 ข้อเสนอแนะสำหรับการนำกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสรรพสิ่งไปใช้งานจริง

5.4.1.1 อินเทอร์เน็ตประสานสรรพสิ่งมีความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับมาก การใช้งานต้องเชื่อมต่อกับอุปกรณ์อื่น มีอุปกรณ์และรูปแบบการใช้งานที่หลากหลาย การใช้งานกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรสิ่ง จึงต้องปรับให้สอดคล้องกับบริบทการใช้งานของอุปกรณ์แต่ละชนิด รวมถึงบริบทการใช้งานอินเทอร์เน็ตประสานสรรพสิ่งของแต่ละองค์กรด้วย

5.4.1.2 การใช้กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง ควรปรับใช้ให้สอดคล้องกับนโยบายและวัตถุประสงค์การดำเนินงานขององค์กร

5.4.2 ข้อเสนอแนะสำหรับการทำวิจัยครั้งต่อไป

5.4.2.1 การวิจัยครั้งต่อไป ควรทำการทดสอบการเจาะระบบของอินเทอร์เน็ตประสานสรรพสิ่ง เพื่อพัฒนาความแข็งแกร่งที่มีต่อการถูกโจมตีทางไซเบอร์

5.4.2.2 การทำวิจัยครั้งต่อไป ควรวิเคราะห์ค่าความสัมพันธ์ระหว่างตัวแปรเพื่อแสดงถึงผลลัพธ์ที่เด่นชัดมากยิ่งขึ้น

บรรณานุกรม

ขวัญชนก ศรีมูล, ฐาปนี ฉายากุล, เอมอัชนา นิรันตสุขรัตน์, พนิตา พงษ์ไบูลย์ และ สุขุมาล กิติสิน. (2560). **การศึกษาปรียบเทียบ NETPIE กับแพลตฟอร์ม Internet of Things อื่น**. การประชุมทางวิชาการระดับชาติด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศ ครั้งที่13, 6 - 7 กรกฎาคม 2560, โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพมหานคร. หน้า 680 – 685.

ชลาธิป ทุมกานนท์ และคณะ. (2560). **การประมวลผลบนคลาวนด์ : โครงสร้างพื้นฐานสำหรับ Internet of Things**. วารสารวิชาการมหาวิทยาลัยอีสเทิร์นเอเชียฉบับวิทยาศาสตร์และเทคโนโลยี, ปีที่ 11 ฉบับที่ 1 (มกราคม – เมษายน), หน้า 30 – 37.

ปริญญา หอมอเนก. (2557). **บทวิเคราะห์กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ระดับโลก "NIST's Framework for Improving Critical Infrastructure Cybersecurity" ... โอกาส ภัยคุกคาม และความเสี่ยงที่ผู้บริหารองค์กรต้องตระหนัก.** วารสารสถาบันวิชาการป้องกันประเทศ, ปีที่ 5 ฉบับที่ 2 (กุมภาพันธ์ - พฤษภาคม), หน้า 19 – 30.

พชรอร เพชรสมุทร และมหศักดิ์ เกตุฉ่ำ. (2560). **ระบบป้องกันการโจรกรรมรถจักรยานยนต์โดยใช้เทคนิคการนู้จำใบหน้าผ่านคลาวด์ ภายใต้แนวคิดอินเทอร์เน็ตเพื่อทุกสิ่ง**. การประชุมทางวิชาการระดับชาติด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศ ครั้งที่13, 6 - 7 กรกฎาคม 2560, โรงแรมเซ็นจูรี่ พาร์ค กรุงเทพมหานคร. หน้า 137 – 143.

มหศักดิ์ เกตุฉ่ำ. (ม.ป.ป.). **Internet of Things (IoT)**. (ไฟล์ PowerPoint). ภาควิชาการจัดการเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ.

รัชชานนท์ วาริศร, วันชัย แลเซอะ, วิทยา อินทร์บุญ, สมชาย นามลง และอนุพันธ์ พงษ์สนั่น (2559). **Internet of things**. (เว็บบล็อก). สืบค้นจาก: http://witthyainbun.blogspot.com/p/internet-of-things.html.

รัชชานนท์ วาริศร, วันชัย แลเซอะ, วิทยา อินทร์บุญ, สมชาย นามลง และอนุพันธ์ พงษ์สนั่น (2559). **Internet of things**. (เว็บบล็อก). สืบค้นจาก: http://witthyainbun.blogspot.com/p/internet-of-things.html.

ราชกิจจานุเบกษา. (2560). **ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560**. เล่มที่ 134 ตอนพิเศษ ลงวันที่ 20 ตุลาคม 2560.

สรวิศ บุญมี. (2561). **ความมั่นคงปลอดภัยของ IoT**. วารสารวิชาการมหาวิทยาลัยอีสเทิร์นเอเชีย ฉบับวิทยาศาสตร์และเทคโนโลยี, ปีที่ 11 ฉบับที่ 1 (มกราคม – เมษายน) หน้า 59 – 67.

สราวุฒิ ปีติยาศักดิ์. (2560). **ภัยคุกคามทางไซเบอร์ กับกฎหมายไซเบอร์ไทย.** สืบค้นจาก https://today.line.me/th/pc/article/ภัยคุกคามทางไซเบอร์+กับกฎหมายไซเบอร์ไทย-nZPaZD. [11 กันยายน 2561]

หยาดพิรุณ นาชัยสินธุ์. (2560). **ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย**. วารสารวิจัย มสด สาขามนุษยศาสตร์และสังคมศาสตร์, ปีที่ 13 ฉบับที่ 2 พ.ค.-ส.ค. 2560 หน้า 24-27.

อรพรรณ แซ่ตั้ง, นิสา พุทธนาวงศ์ และ ณัฐพล ธนเชวงสกุล. (2560). **การออกแบบโรงเรือนสำหรับควบคุมอุณหภูมิความชื้น โดยใช้เทคนิคอินเทอร์เน็ตของสรรพสิ่ง เพื่อส่งเสริมการเพาะเลี้ยงเห็ดแครง**. วารสารการอาชีวะและเทคนิคศึกษา, ปีที่ 7 ฉบับที่ 13 (มกราคม – มิถุนายน). หน้า 87 – 97.

โอฬาร เชี่ยวชาญ และ อนุกิจ เสาร์แก้ว. (2560). **การบูรณาการประยุกต์ใช้ RFID (Radio Frequency Identification) และ IoT (Internet of thing) ผ่านระบบคลาวด์ (Cloud Computing) สำหรับการจัดการโลจิสติกส์**. วารสารวิชาการคณะเทคโนโลยีอุตสาหกรรม มหาวิทยาลัยราชภัฏลำปาง, ปีที่ 10 ฉบับที่ 2 (กรกฎาคม – ธันวาคม). หน้า 109 – 119.

ACM U.S. Public Policy Council and ACM Europe Council Policy Committee. (2017). **Statement on Internet of Things Privacy and Security** (Online). Available: https://www.acm.org/binaries/content/assets/publicpolicy/2017_joint_statement_iotprivacysecurity.pdf

Alok Kumar Pathak. (2017). **Security Challenges in Internet of Things (IoT)**. International Journals of Advanced Research in Computer Science and Software Engineering. ISSN: 2277-128X. (Volume-7, Issue-6). p. 648-652.

Bruce Schneider. (2017). **IoT Cybersecurity: What's Plan B?.** Available: https://www.schneier.com/blog/ archives2017/10/iot_ cybersecuri.html. [26 may 2018]

Christopher J. Alberts and Audrey J. Dorofee. (2001). **OCTAVESM Criteria Version 2.0**. Software Engineering Institute.

Claudio A. Ardagna, Ernesto Damiani, Julian Schütte and Philipp Stephanow, **A Case for IoT Security Assurance.** Internet of Everything Algorithms, Methodologies, Technologies and Perspectives, Springer Nature Singapore Pte Ltd. 2018.

Ebraheim Alsaadi and Abdallah Tubaishat. (2015). **Internet of Things: Features, Challenges, and Vulnerabilities.** International Journal of Advanced Computer Science and Information Technology (IJACSIT). Vol. 4, No. 1, 2015, Page: 1-13, ISSN: 2296-1739.

Elisa Bertino. (2017). **Security and Privacy in the IoT**. The 13th International Conference, Inscrypt, Xian, China, Nov 3-5, 2017, pp.3-10.

ISO27001:2013. Available: ftp://hrm.moph.go.th/iso 27001 /iso-27001.pdf [30 ตุลาคม 2560]

Kui Ren. (2017). **The Dual Role of Smartphones in IoT Security**. The 13th International Confrernce, Inscrypt, Xian, China, Nov 3-5, 2017. pp.21-24.

Liu, Jing & Xiao, Yang & Chen, C. (2012). **Authentication and Access Control in the Internet of Things**. Distributed Computing Systems Workshops (ICDCSW), 2012 32nd, pp. 588-592.

Mengmeng Ge, Jin B. Hong, Walter Guttmann and Dong Seong Kim. (2017). **A framework for automating security analysis of the internet of things**. Journal of Network and Computer Applications, Vol.83 (2017). pp. 12-27.

National Institute of Standards and Technology. **Framework for Improving Critical Infrastructure Cybersecurity**. Version 1.1. 2018.

National Institute of Standards and Technology. (n.d.). **CYBERSECURITY FRAMEWORK.** Available: https://www.nist.gov/cyberframework. [11 September 2018]

Orestis Mavropoulos1, Haralambos Mouratidis, Andrew Fish, Emmanouil Panaousis, and Christos Kalloniatis. (2017). **A Conceptual model to support security analysis in the internet of things**. Computer Science and Information Systems. Vol. 14(2), pp. 557-578.

Oracevic, Alma & Dilek, Selma & Ozdemir, Suat. (2017). **Security in Internet of Things: A Survey**. IEEE ISNCC 2017: IEEE International Symposium on Networks, Computers and Communications, 16 – 18 May 2017, Marrakech – Morocco.

Ritesh Mehta. (2017). How the IoT will explode at 2020. Available: https://customerthink .com/how-the-iot-will-explode-at-2020/. [26 may 2018]

Sergio F. Ochoa, Giancarlo Fortino and Giuseppe Di Fatta. (2017). **Cyber-physical systems, internet of things and big data.** Future Generation Computer Systems, Vol. 75(2017), pp. 82-84.

Santhosh Krishna B V and Gnanasekaran T. (2017). **A Systematic Study of Security Issues in Internet-of-Things (IoT)**. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). Feb 10-11, 2017, SCAD Institute of Technology, Palladam, pp. 107-111.

Tokushi Nakashima. (2018). **Creating credit by making use of mobility with FinTech and IoT.** IATSS Research, 42(2018). 61-66.

TRIPWIRE GUEST AUTHORS. (2016). **IoT / IoE: When It's Got an IP Address, It Will Get Hacked** (online). Available: https://www.tripwire.com/state-of-security/featured/iot-ioe-when-its-got-an-ip-address-it-will-get-hacked/, [26 may 2018]

Wei Liang, Jing Long, Dafang Zhang, Xiong Li and Yin Huang. (2018). **Study on IP Protection Techniques for Integrated Circuit in IOT Environment**. Springer Nature Singapore Pte Ltd. 2018.

ภาคผนวก ก
แบบสอบถามเพื่อการวิเคราะห์ความเสี่ยงของภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง

แบบสอบถามเพื่อการวิเคราะห์ความเสี่ยงของภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง (Internet of Things)

<u>คำชี้แจง</u>

แบบสอบถามนี้ได้จัดทำขึ้นเพื่อสอบถามความคิดเห็นของท่านเกี่ยวกับอินเทอร์เน็ตประสานสรรพสิ่ง(Internet of Things : IoT) ผู้วิจัยใคร่ขอความร่วมมือในการตอบแบบสอบถามโดยขอความกรุณาท่านให้ข้อมูลหรือแสดงความคิดเห็นที่ตรงกับความเป็นจริงมากที่สุด ข้อมูลที่ได้จะนำไปใช้ประกอบการศึกษาวัยทางวิชาการเท่านั้น ผู้วิจัย ขอรับรองว่าข้อมูลที่ได้จากแบบสอบถามจะไม่มีผลกระทบหรือก่อให้เกิดความเสียหายกับท่านหรือผู้ที่เกี่ยวข้องแต่ประการใด ข้อคำถามในแบบสอบถาม แบ่งออกเป็น 3 ส่วน คือ

ส่วนที่ 1 ข้อมูลทั่วไปเกี่ยวกับผู้ตอบแบบสอบถาม

ส่วนที่ 2 ความคิดเห็นเกี่ยวกับความเสี่ยงของภัยคุกคามทางไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง

ตอนที่ 3 ความคิดเห็นและข้อเสนอแนะอื่น ๆ

นิยามศัพท์ที่เกี่ยวข้อง

อินเทอร์เน็ตประสานสรรพสิ่ง (Internet of things, IoT) คือ สภาพแวดล้อมที่ประกอบด้วยอุปกรณ์ต่างๆ มีการถ่ายโอนข้อมูลร่วมกันผ่านเครือข่าย โดยไม่จำเป็นต้องใช้ปฏิสัมพันธ์ระหว่างบุคคลกับบุคคลหรือระหว่างบุคคลกับคอมพิวเตอร์ พัฒนามาจากเทคโนโลยีไร้สาย (wireless technology) ระบบเครื่องกลไฟฟ้าจุลภาค (micro-electromechanical systems : MEMS) และอินเทอร์เน็ต ซึ่งคำว่า Things หมายถึง อุปกรณ์ต่างๆ ที่อ้างอิงได้ด้วยเลขไอพี (IP address) และมีความสามารถในการถ่ายโอนข้อมูลระหว่างกันได้ผ่านเครือข่าย ทั้งนี้ Internet of Things ก็คือเทคโนโลยีที่ทำให้อุปกรณ์ต่างๆ สามารถแลกเปลี่ยนข้อมูลกันได้ผ่านเครือข่ายอินเทอร์เน็ต

ผู้วิจัย

นายวิลาส วิถีไพร อีเมล : natforr@mail.com โทรศัพท์ 08-1860-1524

นักศึกษา หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

การแปลผล แบ่งเป็น 5 ระดับ ดังต่อไปนี้

5	หมายถึง	ระดับมากที่สุด
4	หมายถึง	ระดับมาก
3	หมายถึง	ระดับปานกลาง
2	หมายถึง	ระดับน้อย
1	หมายถึง	ระดับน้อยที่สุด

ขอขอบพระคุณเป็นอย่างสูงในความร่วมมือด้วยดีของท่านมา ณ โอกาสนี้

ตอนที่ 1 สถานภาพทั่วไปของผู้ตอบแบบสอบถาม

โปรดทำเครื่องหมาย ✓ ในช่อง ☐ ที่ตรงกับข้อมูลของท่าน เพียงช่องเดียว

1. เพศ ☐ 1) ชาย ☐ 2) หญิง
2. อายุ ☐ 1) 20-30 ปี ☐ 2) 31-40 ปี ☐ 3) 41-50 ปี ☐ 4) 51-60 ปี
3. ตำแหน่ง ☐ 1) เจ้าหน้าที่ระดับปฏิบัติการ ☐ 2) หัวหน้าฝ่าย ☐ 3) หัวหน้าแผนก ☐ 4) ผู้อำนวยการ
4. ระยะเวลาที่ปฏิบัติงาน ☐ 1) น้อยกว่า 1 ปี ☐ 2) 1-5 ปี ☐ 3) 5-10 ปี ☐ 3) มากกว่า 10 ปี
5. ท่านเคยประสบภัยคุกคามทางไซเบอร์หรือไม่ ☐ 1) เคย ☐ 2) ไม่เคย

ตอนที่ 2 ระดับความคิดเห็นของผู้ใช้เพื่อการวิเคราะห์ภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง

โปรดทำเครื่องหมาย ✓ ในช่อง ที่ตรงกับระดับความเห็นของท่านมากที่สุด

หัวข้อแบบสอบถามเพื่อการวิเคราะห์ความเสี่ยงของภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง	ระดับความเห็น				
	5	4	3	2	1
1. การระบุถึงภัยคุกคาม (Identify)					
1.1 มีการกำหนดกลยุทธ์ด้านภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง					
1.2 ผู้บริหารให้ความสำคัญนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง					
1.3 มีการจัดทำบัญชีสินทรัพย์อุปกรณ์อินเทอร์เน็ตประสานสรรพสิ่งอย่างโปร่งใส					
1.4 มีการระบุภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อการปฏิบัติงานของหน่วยงานโดยตรง					

หัวข้อแบบสอบถามเพื่อการวิเคราะห์ความเสี่ยงของภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง	ระดับความเห็น				
	5	4	3	2	1
1.5 มีการประเมินความเสี่ยงด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อการใช้งานอินเทอร์เน็ตประสานสรรพสิ่งของหน่วยงาน					
2. การป้องกัน (Protect)					
2.1 มีการควบคุมการเข้าถึงการใช้งานอุปกรณ์อินเทอร์เน็ตประสานสรรพสิ่ง					
2.2 มีการกำหนดสิทธิ์การใช้งานอุปกรณ์อินเทอร์เน็ตประสานสรรพสิ่ง					
2.3 มีการอบรมเพื่อพัฒนาความรู้ ความสามารถด้านความมั่นคงปลอดภัยทางไซเบอร์ให้แก่บุคลากร					
2.4 มีการสร้างความตระหนักให้บุคลากรใช้งานอุปกรณ์อินเทอร์เน็ตประสานสรรพสิ่งอย่างมั่นคงปลอดภัย					
2.5 มีการติดตั้งเทคโนโลยีด้านความมั่นคงปลอดภัยในอุปกรณ์อินเทอร์เน็ตประสานสรรพสิ่ง					
3. การตรวจพบ (Detect)					
3.1 มีการตรวจพบเหตุการณ์ผิดปกติในการใช้งานอุปกรณ์อินเทอร์เน็ตประสานสรรพสิ่งอย่างทันถ่วงที					
3.2 มีการสังเกตการณ์ในระหว่างการใช้งานอุปกรณ์อินเทอร์เน็ตประสานสรรพสิ่งและบันทึกไว้					
3.3 มีการกำหนดกระบวนการดำเนินงานเพื่อตรวจจับภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง					
4. การรับมือ (Respond)					
4.1 มีการวางแผนเพื่อรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง					
4.2 มีความร่วมมือกับหน่วยงานที่เกี่ยวข้องเพื่อรับมือภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง					

หัวข้อแบบสอบถามเพื่อการวิเคราะห์ความเสี่ยงของภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง	ระดับความเห็น				
	5	4	3	2	1
4.3 มีวิธีการแก้ปัญหาเพื่อบรรเทาความเสียหายจากเหตุการณ์ภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง					
4.4 มีการวิเคราะห์เพื่อคาดการณ์ภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่งที่อาจเกิดขึ้นได้					
4.5 มีการปรับปรุงกระบวนการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง					
5. การกู้คืน (Recover)					
5.1 มีการวางแผนเพื่อกู้คืนข้อมูลหลังเหตุการณ์ภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง					
5.2 มีการปรับปรุงกระบวนการกู้คืนข้อมูลหลังเหตุการณ์ภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง					
5.3 มีความร่วมมือกับหน่วยงานที่เกี่ยวข้องเพื่อคงสภาพความสมบูรณ์ของข้อมูลหลังเหตุการณ์ภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง					

ตอนที่ 3 ความคิดเห็นและข้อเสนอแนะอื่น ๆ

.....

.....

.....

.....

ผู้วิจัย ขอกราบขอบพระคุณที่ท่านได้กรุณาเสียสละเวลาในการตอบแบบสอบถาม

แบบสอบถามเชิงคุณภาพ

เรื่อง **การวิเคราะภัยคุกคามทางไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง**

เพื่อใช้สำหรับการศึกษา

ในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

ส่วนที่ 1 ข้อมูลผู้ตอบแบบสอบถาม

ชื่อ-นามสกุล .....

เพศ .....

อายุ .....

สถานที่ทำงาน .....

ตำแหน่ง .....

ประสบการณ์ทำงานที่เกี่ยวข้อง

.....

.....

.....

ผู้วิจัย นายวิลาส วิถีไพร

นักศึกษาหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

อีเมล : natforr@gmail.com โทร: 081-860-1524

ที่ปรึกษางานวิจัย ศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง อีเมล : prasong.pr@spu.ac.th

ส่วนที่ 2 คำถามเกี่ยวกับมุมมองด้านภัยคุกคามไซเบอร์ในอินเทอร์เน็ตประสานสรรพสิ่ง

(จำนวน 7 ข้อ)

ข้อที่ 1 ในมุมมองของท่าน ปัจจุบันอินเทอร์เน็ตประสานสรรพสิ่ง (Internet of Things : IoT) มีความสำคัญอย่างไร

.....

.....

.....

.....

ข้อที่ 2 ในมุมมองของท่าน ความเสี่ยงด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง (Internet of Things : IoT) เป็นอย่างไร มีอะไรบ้าง

.....

.....

.....

.....

ข้อที่ 3 ในมุมมองของท่าน ภัยคุกคามด้านไซเบอร์ที่มีผลต่ออินเทอร์เน็ตประสานสรรพสิ่ง (Internet of Things : IoT) เป็นอย่างไร มีอะไรบ้าง

.....

.....

.....

.....

ข้อที่ 4 ในมุมมองของท่าน ความเป็นไปได้ในการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง (Internet of Things : IoT) ควรเป็นอย่างไร

.....

.....

.....

.....

ข้อที่ 5 ในมุมมองของท่าน การพัฒนาเตรียมบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง (Internet of Things : IoT) ควรเป็นอย่างไร

.....

.....

.....

.....

ข้อที่ 6 ในมุมมองของท่าน โดยภาพรวม ปัจจุบัน ความมั่นคงปลอดภัยไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง (Internet of Things : IoT) อยู่ในระดับใด มีความพร้อมแค่ไหน

.....

.....

.....

.....

ข้อที่ 7 ในมุมมองของท่าน การเตรียมความพร้อมเพื่อรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์ สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง(Internet of Things : IoT) ควรดำเนินการอย่างไร

.....

.....

.....

.....

ภาคผนวก ข

ผลงานตีพิมพ์

บทคัดย่อผลงานนำเสนอในการประชุมวิชาการ (Conference) จำนวน 2 รายการ

[1] วิลาส วิถีไพร, เอกฉัตร บ่ายคล้อย และประสงค์ ปราณีตพลกรัง, “**การวิเคราะห์ภัยคุกคามทางไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง**,” การประชุมวิชาการระดับชาติและนานาชาติประจำปี 2561, 12 กรกฎาคม 2561 ณ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี.

Abstract

The purpose of the research is to analyze the risks and cyber threats for Internet of things (IoT) by conducting qualitative and quantitative researches. Samples are 7 IoT experts and Staff of 40 people in engineering and planning division of Phetchaburi Provincial Electricity Authority Regional 1 (Southern). The method of data collection proceeding by the interview and the questionnaire. The statistics used in data analysis are percentage, mean and standard deviation.

For qualitative researches, found that the IoT obtained high-risk of cyber threats. Because It still happens at the beginning. There is no standard for maintaining good security. For quantitative researches, we found that the score of the overall opinions about the identification of the security measures was at the high level, the score of the overall opinions about the protection of cyber threats was at the moderate level, the score of the overall opinions about cyber threats detection was at the moderate level, the score of the overall opinions about the respond of cyber threats was at the moderate level, and score of the overall opinions about data recovery after cyber threats mattered was at the moderate level.

[2] Wilas Witheeprai, Ekkachat Baikloy and Prasong Praneetpolgrang, **"The Development of Cybersecurity Framework for Internet of Things,"** The 6th International Conference on Robotics, Informatics and Intelligent Control Technology, 4 – 6 September 2018, Asia Hotel Bangkok, Thailand.

Abstract

Internet of things is performing an important role in digital society. In the same time, there are threats in the high level. This is because there is no standard for cybersecurity, obviously. This research aims to develop a cybersecurity framework for Internet of things. The researcher analyzed the cyber threats in the Internet of things from in-depth with experts is interviewed and by samples of closed-end questionnaires from the engineering and planning of Phetchaburi Provincial Electricity Authority Area 1 (Southern). Based on data analysis and some references, the cybersecurity framework of the National Institute of Standards and Technology, USA. Researchers have developed cybersecurity framework for Internet of things, moreover; We have also expanded some applications for the risk of cybersecurity of Internet of things evaluation. This will enable organizations to better prepare and improve their cybersecurity policies for Internet of things use.

ประวัติผู้วิจัย

ชื่อ-ชื่อสกุล นายวิลาส วิถีไพร

วัน เดือน ปี เกิด 26 พฤศจิกายน 2525

ที่อยู่ปัจจุบัน 217 ซ.รามอินเทรา 27 แขวงอนุสาวรีย์ เขตบางเขน กรุงเทพ 10220

วุฒิการศึกษา พ.ศ 2548 บริหารธุรกิจบัณฑิต สาขาวิชาการจัดการทั่วไป
มหาวิทยาลัยธุรกิจบัณฑิตย์

ประสบการณ์การทำงาน พ.ศ. 2558 - ปัจจุบัน
นักวิชาการศึกษาปฏิบัติการ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
พ.ศ. 2557 – 2558
นักวิเคราะห์นโยบายและแผน กรมส่งเสริมสหกรณ์
พ.ศ. 2552 – 2557
นักวิชาการศึกษาปฏิบัติการ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
พ.ศ. 2548 – 2549
Cutomer Service บริษัท บัตรเครดิตกรุงศรีอยุธยา จำกัด

ผลงานวิชาการที่ได้รับการตีพิมพ์

[1] วิลาส วิถีไพร, เอกฉัตร บ่ายคล้อย และประสงค์ ปราณีตพลกรัง, **“การวิเคราะห์ภัยคุกคามทางไซเบอร์สำหรับอินเทอร์เน็ตประสานสรรพสิ่ง,”** การประชุมวิชาการระดับชาติและนานาชาติประจำปี 2561, 12 กรกฎาคม 2561 ณ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี.

[2] Wilas Witheeprai, Ekkachat Baikloy and Prasong Praneetpolgrang, **“ The Development of Cybersecurity Framework for Internet of Things,”** The 6th International Conference on Robotics, Informatics and Intelligent Control Technology, 4 – 6 September 2018, Asia Hotel Bangkok, Thailand.