บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเป็นยุคที่พัฒนาต่อจากยุคสังคมอุตสาหกรรม มาเป็นยุคอินเทอร์เน็ตและดิจิทัล ซึ่งเทคโนโลยีดิจิทัลได้กลายเป็นโครงสร้างพื้นฐานที่สำคัญอย่างยิ่งขององค์กร ทำให้ผู้คนสามารถติดต่อสื่อสารข้อมูลถึงกันได้อย่างสะดวกและรวดเร็วไม่ว่าจะอยู่ ณ ที่ใดในโลก ทั้งนี้ โครงสร้างพื้นฐานทางเศรษฐกิจและสังคมของศตวรรษที่ 21 (Bryndin, 2018) ประกอบด้วยข้อมูลดิจิทัลและเทคโนโลยีดิจิทัลเป็นหลัก เมื่อโลกเข้าสู่ยุคที่ทุกสิ่งอย่างได้ถูกขับเคลื่อนด้วยดิจิทัล (Digital-Driven) (Härting, et al., 2018) เทคโนโลยีดิจิทัลจึงมีบทบาทความสำคัญต่อการพลิกฟื้น ปรับปรุง และยกระดับประสิทธิภาพการทำงานขององค์กรเป็นอย่างมาก เทคโนโลยีดิจิทัลไม่ได้เป็นเพียงเครื่องมือสนับสนุนการทำงานเช่นในอดีตที่ผ่านมาอีกต่อไป หากแต่ยังหลอมรวมเข้ากับวิถีชีวิตของผู้คนในทุก ๆ มิติ ไม่ว่าจะเป็นมิติทางการเมืองเศรษฐกิจ สังคมจิตวิทยา วิทยาศาสตร์และเทคโนโลยี เราจะพบว่า สถานการณ์โลกมีการเปลี่ยนแปลงอย่างรวดเร็ว โดยเฉพาะเทคโนโลยีได้มีการดิสรัปชันหรือเปลี่ยนฉับพลัน (Disruption) อยู่เสมอ (Dmitry, et al., 2018)

ตามแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้เน้นถึงการเป็นดิจิทัลไทยแลนด์ (Digital Thailand) ที่จะทำให้ประเทศไทยสามารถสร้างสรรค์ และใช้ประโยชน์จากเทคโนโลยีดิจิทัลอย่างเต็มศักยภาพในการพัฒนาโครงสร้างพื้นฐาน นวัตกรรม ข้อมูล ทุนมนุษย์ และทรัพยากรอื่นใด เพื่อขับเคลื่อนการพัฒนาเศรษฐกิจและสังคมของประเทศไปสู่ความมั่นคง มั่งคั่ง และยั่งยืน ทั้งนี้ การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของประเทศไทยได้สอดคล้องกับการจัดทำยุทธศาสตร์ชาติ 20 ปี (สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ, 2561) โดยกำหนดยุทธศาสตร์ไว้ 6 ด้าน คือ 1) พัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ 2) ขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล 3) สร้างสังคมคุณภาพที่ทั่วถึงเท่าเทียมด้วยเทคโนโลยีดิจิทัล 4) ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล 5) พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล และ 6) สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

จะเห็นได้ว่าการเปลี่ยนแปลงอย่างรวดเร็วและรุนแรงที่เกิดขึ้นในยุคดิจิทัลนี้ ได้ส่งผลกระทบต่อสิ่งต่าง ๆ รอบด้าน ไม่ว่าจะเป็นในภาคสังคม การเมือง เศรษฐกิจ และการเงิน รวมไปถึงธุรกิจทั้งภายในประเทศและต่างประเทศต่างก็ตกอยู่ภายใต้กระแสของการเปลี่ยนแปลงของโลกด้วยกันทั้งสิ้น การดิสรัปชันทางดิจิทัลนั้นเป็นการปฏิรูปหรือเปลี่ยนแปลงที่เกิดจากการประยุกต์ใช้เทคโนโลยีดิจิทัลและโมเดลธุรกิจแบบใหม่ เพื่อให้สามารถส่งผลกระทบต่อมูลค่าของผลิตภัณฑ์และบริการที่มีอยู่ในภาคธุรกิจ องค์กรต่าง ๆ (Nieuwenhuis, et al., 2018) โดยเฉพาะองค์กรทางธุรกิจจึงต้องปรับตัวให้เข้าสู่การเปลี่ยนแปลงทางเทคโนโลยีดิจิทัล (Digital Transformation) ดังนั้นแล้ว การเปลี่ยนผ่านทางดิจิทัลจึงเป็นเรื่องที่ทุกองค์กรต้องตระหนักและดำเนินการเพื่อความอยู่รอด ยิ่งไปกว่านั้น เมื่อเทคโนโลยีดิจิทัลมีความก้าวหน้าอย่างรวดเร็ว การเข้าถึงอินเทอร์เน็ตสามารถทำได้ทุกที่ทุกเวลา ประเทศของเราต้องเผชิญกับภัยคุกคามในรูปแบบใหม่ที่เรียกว่าภัยคุกคามทางไซเบอร์ ทำให้เกิดความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ การก่อการร้ายไซเบอร์ การหลอกลวงและอื่น ๆ มีมากขึ้น การระบุและวิเคราะห์ภัยคุกคามที่ชัดเจนดังเช่นในอดีตทำได้ยาก ความมั่นคงปลอดภัยด้านไซเบอร์จึงเป็นเรื่องสำคัญยิ่งในโลกยุคดิจิทัล

การขยายตัวทางธุรกิจท่ามกลางการแข่งขันที่สูงขึ้น และเทคโนโลยีที่ผันเปลี่ยนไปอย่างรวดเร็วนั้น ประเทศไทยมีความต้องการพัฒนาอุตสาหกรรมไทยให้สามารถตอบสนองการเปลี่ยนแปลงเทคโนโลยีหรือแนวโน้มการค้าโลก พัฒนาโครงสร้างพื้นฐานด้านดิจิทัลและการ มุ่งสู่การเป็นประเทศอัจฉริยะ การอำนวยความสะดวกเพื่อสนับสนุนธุรกิจการค้า การนำเข้าส่งออก และระบบโลจิสติกส์ในรูปแบบดิจิทัล โดยพัฒนาการค้าสู่รูปแบบพาณิชย์อิเล็กทรอนิกส์ ภายใต้โครงสร้างพื้นฐานด้านดิจิทัล ในขณะเดียวกัน การจัดการเกี่ยวกับระบบโซ่อุปทานหรือ ซัพพลายเชนที่ได้นำมาใช้ในองค์กร ได้กลายมาเป็นระบบที่ต้องทำงานอยู่ภายใต้เครือข่ายคอมพิวเตอร์ที่มีการรับส่งข้อมูลทางอิเล็กทรอนิกส์มากขึ้น นับตั้งแต่ปี พ.ศ. 2543 (หรือ ปี ค.ศ. 2000) เป็นต้นมา จะเห็นได้ว่าเทคโนโลยีสารสนเทศหรือเทคโนโลยีดิจิทัลได้มีความก้าวหน้าขึ้นอย่างก้าวกระโดด โดยส่วนมากจะเป็นการประยุกต์เพื่อนำมาใช้ในการสนับสนุนการดำเนินงานทางด้านธุรกิจ จุดเริ่มต้นของการพัฒนาก็เพื่อที่จะนำมาช่วยสนับสนุนการดำเนินงานในแต่ละบริษัทหรือองค์กรเท่านั้น ซึ่งผลที่เกิดขึ้นได้ทำให้การดำเนินงานภายในบริษัทหรือองค์กรเหล่านั้นมีความคล่องตัวและรวดเร็วมากยิ่งขึ้น แต่เนื่องจากความซับซ้อนทางด้านธุรกิจมีมากขึ้นในปัจจุบันจึงได้มีการพัฒนาเทคโนโลยี เพื่อให้แต่ละธุรกิจหรือบริษัทต่าง ๆ ในโซ่อุปทานสามารถที่จะทำงานร่วมกัน (Collaboration) จึงเป็นผลทำให้เกิดมีการใช้ข้อมูลร่วมกัน (Information Sharing) รวมไปถึงการเชื่อมต่อธุรกิจ (Business Connectivity) ระหว่างกันในโซ่อุปทานได้

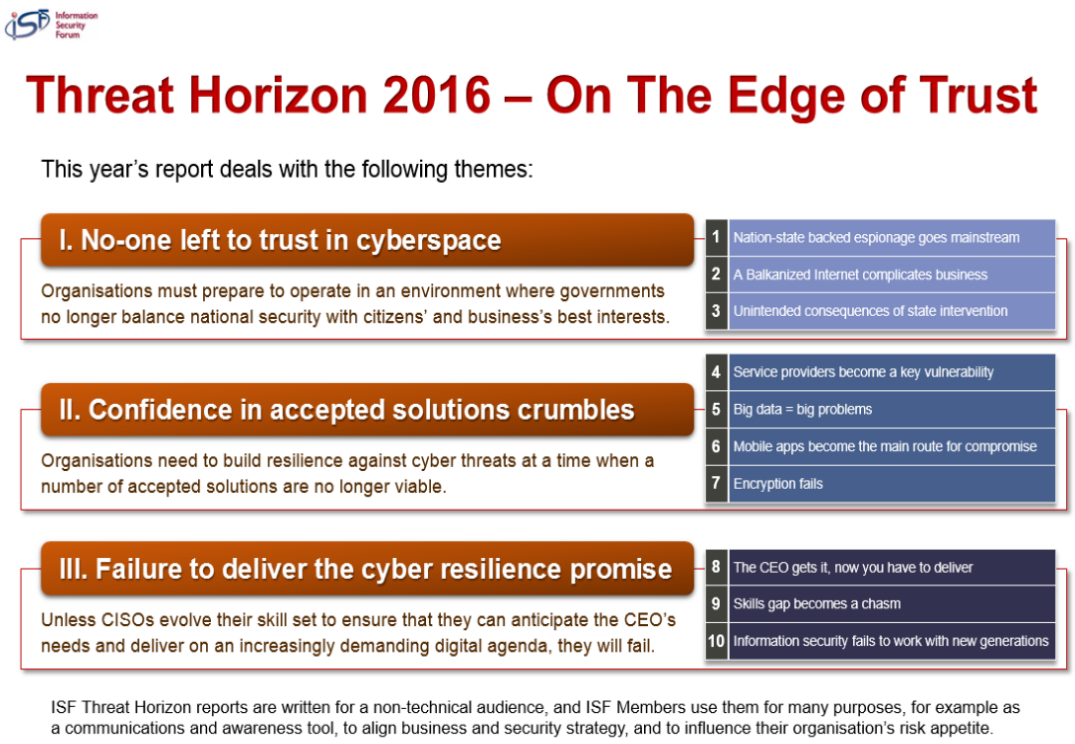
ด้วยเหตุนี้การดำเนินกิจกรรมในด้านต่าง ๆ ที่เกิดขึ้นในภายในระบบโซ่อุปทานโดยเฉพาะระบบโซ่อุปทานภายใต้โครงสร้างพื้นฐานดิจิทัลนั้น จึงจำเป็นที่จะต้องสร้างมาตรฐานของกระบวนการทางธุรกิจร่วมกัน จะต้องมีการเชื่อมต่อและแลกเปลี่ยนข้อมูลระหว่างกัน รวมไปถึงจะต้องมีการสื่อสารระหว่างกันเพิ่มมากขึ้น (Büyüközkan, 2018) จากประเด็นที่ได้กล่าวมาทั้งหมดเหล่านี้ เมื่อมีการลงมือปฏิบัติการเพื่อให้เกิดผลของการดำเนินงานในระบบโซ่อุปทานดิจิทัลย่อมจะทำให้เกิดความเสี่ยง (Dmitry, et al., 2018) ความเสี่ยงในที่นี้ส่วนใหญ่มักเป็น ภัยคุกคาม (Threat) ช่องโหว่ หรือ จุดอ่อน (Vulnerability) ผลกระทบ (Impact) และโอกาส (Likelihood) ที่จะเกิดขึ้นในระบบโซ่อุปทานได้ทั้งสิ้น ซึ่งเป็นสาเหตุที่ทำให้เกิดการโจมตีจากผู้ไม่หวังดีได้ โดยเหตุผลที่ทำให้เกิดช่องโหว่ของหรือจุดอ่อนของระบบอันเป็นเหตุให้เกิดการโจมตีได้ ส่วนหนึ่งก็เกิดมาจากงานที่ได้มีการประยุกต์นำเอาเทคโนโลยีดิจิทัลมาใช้เพื่อสนับสนุนการทำงานในระบบโซ่อุปทาน งานในลักษณะดังกล่าวได้ถูกออกแบบมาเพื่อใช้ข้อมูลร่วมกันที่เป็นข้อมูลแบบดิจิทัลหรืออิเล็กทรอนิกส์มากขึ้น

การโจมตีทางไซเบอร์ (Cyber Attack) (Warren Matthew et al., 2000; Zobel Christopher, 2013) รวมไปถึงอาชญากรรมทางไซเบอร์ (Cyber Crime) เป็นส่วนหนึ่งของภัยคุกคามที่เป็นความเสี่ยงทางไซเบอร์ (Cyber Risk) ที่เริ่มเห็นชัดมากขึ้นในปัจจุบัน อันเป็นผลมาจากการใช้งานจากเทคโนโลยีสารสนเทศและการสื่อสารที่มีความก้าวหน้าเป็นผลทำให้เกิดปัญหาภัยคุกคามทางไซเบอร์ ในขณะที่ปัญหาดังกล่าวนี้ส่วนมากจะเป็นปัญหาที่เกี่ยวกับความมั่นคงปลอดภัยข้อมูลคอมพิวเตอร์ โดยเฉพาะภัยที่มาจากการติดต่อสื่อสารผ่านเครือข่ายอินเทอร์เน็ต ที่นับวันจะยิ่งทวีความรุนแรงและพัฒนารูปแบบของภัยคุกคามที่หลากหลายมากขึ้น และภัยคุกคามทางไซเบอร์ (Cyber Threats) ได้เพิ่มระดับความรุนแรงและมีความซับซ้อนในการโจมตีมากขึ้นเป็นลำดับซึ่งจะมีผลต่อธุรกิจอย่างร้ายแรง (Levi, M., 2016; Brar, H. S., & Kumar, G., 2018; Rusi, T., & Lehto, M., 2017; Gaudenzi, B., & Siciliano, G., 2017; Papastergiou, S., & Polemi, N., 2018)

อุปกรณ์หรือเครื่องมือที่สามารถเชื่อมต่อกับระบบอินเทอร์เน็ตที่ได้ถูกนำมาใช้งานในปัจจุบัน (Lee, J. et al., 2016; Hwang, G. J. et al., 2017) มีความหลากหลายและมีขายทั่วไปตามท้องตลาด อุปกรณ์หรือเครื่องมือดังกล่าวได้แก่ เครื่องคอมพิวเตอร์ โน้ตบุ๊ก โมไบล์โฟนหรือโทรศัพท์เคลื่อนที่ แท็บเล็ต สมาร์ตโฟน หรืออุปกรณ์พกพาต่าง ๆ โดยที่อุปกรณ์เหล่านี้สามารถที่จะนำมาใช้งานในเพื่อทำให้การทำงานมีความคล่องตัวและสะดวกสบายมากขึ้น แต่ผลที่ตามมาสำหรับการใช้เทคโนโลยีการสื่อสารผ่านอุปกรณ์ที่ทันสมัยเหล่านี้ก็คือ การที่ต้องเผชิญกับภัยคุกคามทางไซเบอร์อย่างที่หลีกเลี่ยงไม่ได้และจากการเพิ่มขึ้นของการนำเอาระบบเทคโนโลยีสารสนเทศมาใช้นี้ เป็นผลให้นำมาสู่ความเสี่ยงทางไซเบอร์ที่เพิ่มขึ้นเช่นเดียวกัน ซึ่งมีผลกระทบ

ต่อระบบโซ่อุปทานดิจิทัลทั้งในแง่ของผลิตภัณฑ์หรือบริการที่ได้ถูกส่งมอบให้กับลูกค้าและการดำเนินกิจกรรมต่าง ๆ ในโซ่อุปทานดิจิทัล (Herrera, A. V. et al., 2017; Baillette, P. et al., 2018)

จากรายงานแนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ สำหรับปี 2016 “Threat Horizon 2016” รายงานในธีมหัวข้อ “On The Edge of Trust” โดย Information Security Forum (2016) ได้รายงานสรุปทิศทางในเชิงลบ เป็นภัยความเสี่ยง 3 ประเด็นหลัก คือ (1) ไม่มีใครน่าไว้วางใจในไซเบอร์อีกต่อไป (2) ความเชื่อมั่นในระบบหรืองานประยุกต์การรักษาความมั่นคงปลอดภัยในแนวทางที่ยอมรับโดยทั่วไปเสื่อมสลาย ต้องคิดหาแนวทางใหม่ และ (3) ความล้มเหลวต่อการรักษาระดับการให้บริการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ดังภาพประกอบที่ 1.1

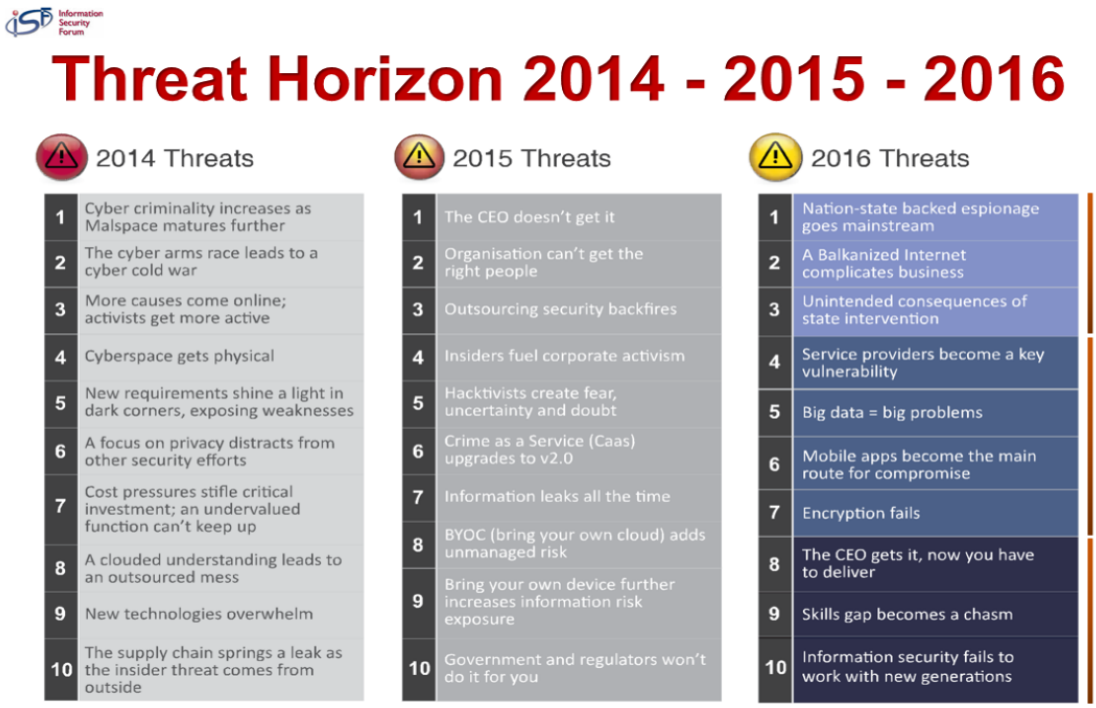


ภาพประกอบที่ 1.1 ภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ (Threat Horizon 2016 – On The Edge of Trust)

ที่มา : The Information Security Forum, ISF Threat Horizon 2016 Executive Summary

โดยในรายงานได้มีการสรุปเปรียบเทียบถึงความรุนแรงของภัยคุกคามไซเบอร์ ที่มีมาตั้งแต่ปี 2014 จนถึงปี 2016 โดยในรายงาน Threat Horizon แสดงให้เห็นว่า ความรุนแรงของภัยคุกคามไซเบอร์ยังคงมีอย่างต่อเนื่อง องค์กรต่าง ๆ ไม่มีความสามารถในการปรับตัวและรับมือ

ในส่วนของประธานบริหาร (Chief Executive Officer (CEO)) เริ่มจะมีความเข้าใจถึงผลของภัยคุกคามดังกล่าว แต่ผู้บริหารที่รับผิดชอบไม่สามารถจะให้ข้อมูลแผนงานและแนวทางดำเนินการได้ ประกอบกับมาตรการความมั่นคงปลอดภัยที่ปฏิบัติใช้อยู่นั้นไม่เหมาะกับคนรุ่นใหม่ ในขณะที่การใช้งานโปรแกรมประยุกต์ต่าง ๆ ภายในองค์กรหรือบริษัทที่มีอยู่ในปัจจุบัน ได้กลายเป็นภัยคุกคามเสียเอง ทั้งจากการใช้งานจากผู้ให้บริการภายนอก แอปพลิเคชันมือถือ การเข้ารหัสข้อมูล และการจัดการข้อมูลขนาดใหญ่ขององค์กร ตลอดจนบทบาทภาครัฐที่เข้ามาแทรกแซงหรือควบคุมอินเทอร์เน็ต รวมทั้งการสนับสนุนเต็มที่ของภาครัฐในการจารกรรมทางไซเบอร์ ดังภาพประกอบที่ 1.2



ภาพประกอบที่ 1.2 ประเด็นภัยคุกคามความมั่นคงปลอดภัยสารสนเทศเปรียบเทียบปี 2014, 2015, 2016

ที่มา : The Information Security Forum, ISF Threat Horizon 2016 Executive Summary

ล่าสุดจากรายงานของ Threat Horizon 2019 (ISF, 2019) ที่ได้ทำการศึกษาจากองค์กรที่สำคัญ 9 แห่ง ที่อาจจะต้องเผชิญต่อภัยคุกคามที่สำคัญในอีกสองถึงสามปีข้างหน้าอันเป็นผลมาจากการการเปลี่ยนแปลงเทคโนโลยี ภัยคุกคามดังกล่าวได้ถูกกำหนดไว้ภายใต้ สาระสำคัญหลัก ๆ 3 ประการที่จะสะท้อนให้เห็นถึงผลกระทบที่สำคัญที่ควรเกิดขึ้น ซึ่งได้แก่

ประเด็นที่ 1 – การหยุดชะงัก (Disruption) จากการพึ่งพาการเชื่อมต่อที่บอบบาง

ประเด็นที่ 2 – การบิดเบือน (Distortion) ความน่าเชื่อถือในความสมบูรณ์ของข้อมูลจะสูญหายไป

ประเด็นที่ 3 – การเสื่อมสภาพ (Deterioration) เมื่อตัวควบคุมถูกกัดเซาะโดยข้อบังคับและเทคโนโลยี

โลกในปี 2019 จะขึ้นอยู่กับเทคโนโลยีและการเชื่อมต่อทั้งหมดและองค์กรจะต้องใช้เครื่องมือทุกอย่างเพื่อการดำเนินการให้สามารถก้าวข้ามต่อภัยคุกคามที่จะเข้ามาเพื่อการดำเนินไปข้างหน้า โลกในอนาคตจึงจำเป็นต้องที่จะสร้างวัฒนธรรมในการให้ความร่วมมือที่เข้มแข็งกับคนและเวลาที่เหมาะสมเพื่อที่จะทำให้เกิดการมีความส่วนร่วมระหว่างกันในอันที่จะทำให้เกิดความสำเร็จที่จะรับมือต่อภัยคุกคามได้

ภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบันนี้ ได้เริ่มเข้ามาก่อให้เกิดปัญหาอันจะส่งผลกระทบต่อโซ่อุปทานดิจิทัล ที่ไม่ใช่เพียงแต่ในระดับประเทศเท่านั้นแต่ยังจะอาจจะมีผลกระทบต่อโซ่อุปทานดิจิทัลในโลกได้อีกด้วย โดยภัยคุกคามไซเบอร์สามารถเกิดได้ทั้งภายในโซ่อุปทานดิจิทัลและระหว่างโซ่อุปทานดิจิทัล (Lamba, A., 2017; Chhetri, S. R., 2017) ภัยคุกคามดังกล่าวนี้จะแฝงตัวมากับการเติบโตทางด้านเทคโนโลยีดิจิทัลอันเป็นผลมาจากการพัฒนาเครือข่ายระบบอินเทอร์เน็ต โดยการพัฒนาระบบเครือข่ายการสื่อสารข้อมูลที่สามารถเชื่อมต่อกันด้วยระบบเครือข่ายใยแก้วนำแสง การเชื่อมต่อแบบไร้สาย หรือแม้แต่ระบบสื่อสารดาวเทียม จนทำให้โลกถูกเชื่อมต่อกันโดยสมบูรณ์และสามารถส่งข้อมูลด้วยความเร็วเท่าแสง และยังมีแนวโน้มที่จะเพิ่มการเชื่อมโยงให้มากขึ้น (Akinrolabu, O. et al., 2018; Wagner, T. D., et al., 2018) สิ่งที่เป็นปัญหาที่สามารถทำให้อาชญากรทางไซเบอร์สามารถที่จะเข้ามาทำการโจรกรรมข้อมูลภายในบริษัทส่วนหนึ่งก็จะมาจากเทคโนโลยีที่มีใช้อยู่ในท้องตลาดทั่วไปเริ่มมีขีดความสามารถเท่าเทียมกับเทคโนโลยีของหน่วยงานความมั่นคงของประเทศ จึงเป็นเหตุให้อาชญากรทางไซเบอร์มีทางเลือกในการปฏิบัติมากขึ้นและมีความซับซ้อนมากขึ้นขึ้น และเป็นการยากที่จะตรวจจับได้ ยิ่งไปกว่านั้น ในปัจจุบันเราจะเห็นว่าเครื่องมือและคู่มือในการเจาะระบบสารสนเทศก็สามารถพบเห็นได้ทั่วไปในอินเทอร์เน็ตเพียงแค่เราทำการสืบค้นจาก Google ดังที่เคยมีข่าวออกมาว่า เด็กอายุเพียง 10 ขวบ ก็สามารถเจาะระบบของธนาคารทั่วโลกได้ เพื่อขโมยหรือลบข้อมูลสำคัญของธนาคาร (เศรษฐพงค์ มะลิสุวรรณ, 2010)

จากปัญหาของภัยคุกคามไซเบอร์ ที่ส่งผลต่อการดำเนินงานในโซ่อุปทานนั้น ทำให้เห็นตัวอย่างการโจมตีที่เกิดขึ้นอยู่บ่อยครั้ง และจากรายงานสถานการณ์ภัยคุกคามของ Trend Micro ในปี 2015 (TrendMicro, 2015) ได้รายงานว่า “ในช่วงปี 2015 ที่ผ่านมาภัยคุกคามทางไซเบอร์จะ

ประกอบด้วยภัยคุกคามทั้งแบบเก่าและแบบใหม่ ไม่ว่าจะเป็น มัลแวร์ที่แฝงตัวในโฆษณา (Malvertising) และการโจมตีทางไซเบอร์ไปยังช่องโหว่ที่เกิดขึ้น (Zero-Days Attack) ได้กลายมาเป็นภัยคุกคามที่ท้าทายความน่าเชื่อถือในระบบห่วงโซ่อุปทานและแนวทางปฏิบัติที่เหมาะสม” (Bad Ads and Zero-Days : Reemerging Threats Challenge Trust in Supply Chains and Best Practices) นอกจากนี้แอดแวร์ (Adware) ยังครองอันดับสูงสุดในบรรดาภัยคุกคามบนระบบโมไบล์ (Mobile) โดย TrendMicro ตรวจพบภัยคุกคามบน Android มากกว่า 5 ล้านชนิด แอปพลิเคชันที่เป็นอันตรายและมีความเสี่ยงสูง ที่ถูก TrendMicro บล็อกไว้ ส่วนมากมีสาเหตุมาจากแอดแวร์ทั้งสิ้น นักวิจัยของ TrendMicro ยังตรวจพบการใช้ช่องโหว่ใหม่ ๆ เพื่อโจมตีซอฟต์แวร์ของ Adobe โดยใช้มัลแวร์แฝงตัวมาอยู่ในโฆษณาที่สามารถทำงานได้ถึงแม้เหยื่อไม่ได้เยี่ยมชมหรือโต้ตอบกับเว็บไซต์อันตรายก็ตาม นอกเหนือจาก iOS™ และระบบชำระเงิน (Point-of-Sale-PoS) ที่ตกเป็นเป้าหมายการโจมตีอย่างต่อเนื่องแล้ว นอกจากนี้ธุรกิจความงามและสุขภาพก็ได้ตกเป็นเป้าหมายใหม่ที่ต้องเผชิญกับการโจมตีทางไซเบอร์ที่เพิ่มขึ้นอย่างมาก

รายงานข้อมูลจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) ดังแสดงในตารางที่ 1.1 ระบุว่ามีเหตุการณ์จู่โจมจากอาชญากรไซเบอร์เกิดขึ้นถึง 4,300 ครั้งในประเทศไทยตลอดปี 2558 เราจะพบว่าสถิติสูงกว่าปีก่อนหน้า 30% ในจำนวนนี้กว่า 35% มีมัลแวร์เป็นต้นเหตุ

ตารางที่ 1.1 สถิติภัยคุกคามทางไซเบอร์ของประเทศไทย ประจำปี 2558

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	2	0	0	0	0	2	0	0	0	2	1	1	**8**
Availability	0	0	0	0	0	0	0	0	0	0	1	5	**6**
Fraud	75	83	100	90	155	134	113	99	70	67	80	75	**1141**
Information gathering	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Information security	0	0	1	0	0	0	0	0	0	0	0	0	**1**
Intrusion Attempts	83	89	65	27	60	44	63	51	52	59	43	28	**664**
Intrusions	69	76	88	12	78	187	159	83	51	105	42	55	**1005**
Malicious code	104	83	174	143	140	209	192	97	143	119	92	50	**1546**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
รวม	**333**	**331**	**428**	**272**	**433**	**576**	**527**	**330**	**316**	**352**	**259**	**214**	**4371**

ที่มา : https://www.thaicert.or.th/statistics/statistics2015.html

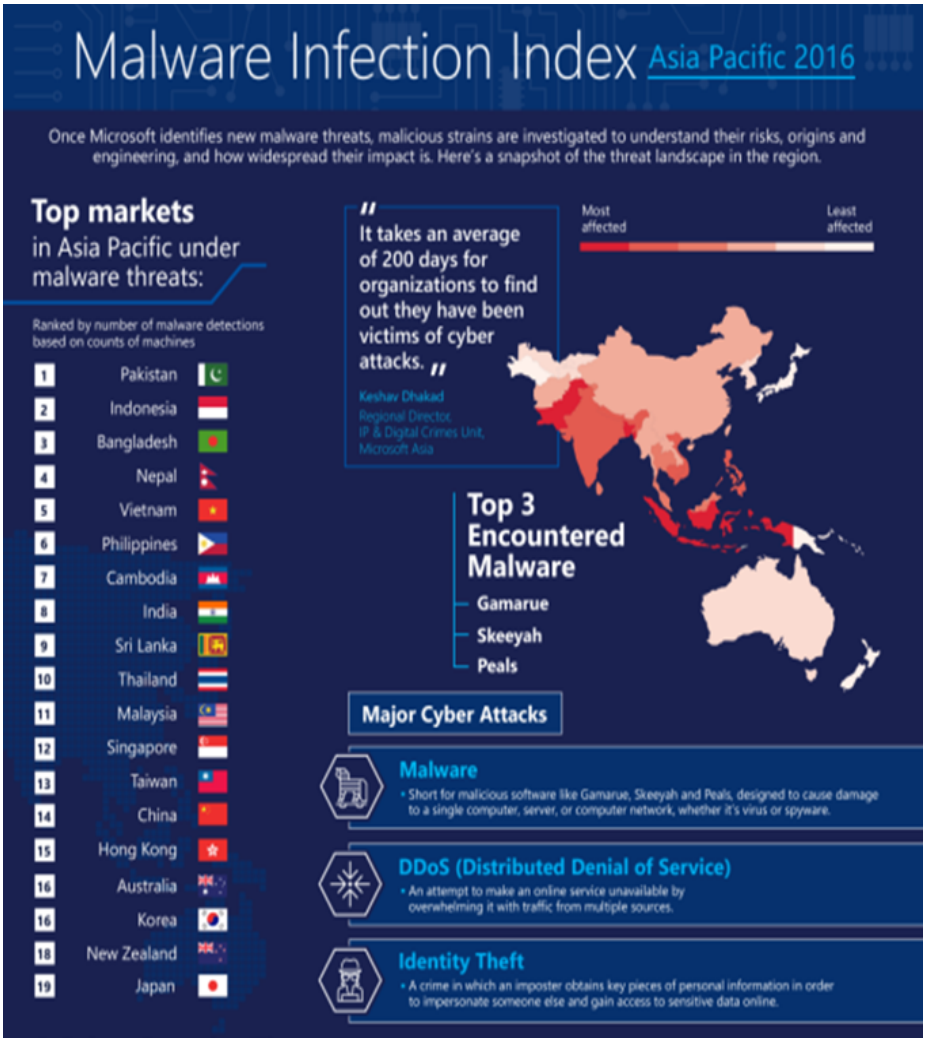
และเนื่องจากแนวโน้มของภัยคุกคามทางด้านความมั่นคงได้มีการเปลี่ยนแปลงอย่างชัดเจนมากขึ้น ฝ่ายตรงข้ามหรือผู้ก่อการร้ายหรือผู้ที่ไม่หวังดี สามารถที่จะทำการโจมตีจุดที่สำคัญอันเป็นหัวใจของโซ่อุปทานได้ โดยผ่านระบบเครือข่ายโทรคมนาคมและคอมพิวเตอร์ ที่มีการใช้งานขององค์กรนั้น ๆ ภัยคุกคามไซเบอร์ เป็นเรื่องที่บริษัทหรือหน่วยงานต่าง ๆ ทั้งที่เป็นของรัฐและเอกชนกำลังเผชิญอยู่ ภัยคุกคามทางไซเบอร์เป็นสิ่งที่สามารถสร้างความเสียหายให้กับระบบคอมพิวเตอร์

ที่มีการใช้งานอยู่ในปัจจุบัน ธุรกรรมใด ๆ ที่เกิดขึ้นในโซ่อุปทานล้วนต้องอาศัยการทำงานผ่านอุปกรณ์ต่าง ๆ ของระบบคอมพิวเตอร์แทบทั้งสิ้น ดังนั้นด้วยเหตุที่มีอุปกรณ์มากมายที่บริษัทต่าง ๆ ได้นำมาใช้เพื่อการทำงาน ก็เท่ากับว่าเป็นการเพิ่มช่องทางให้กับผู้ที่ไม่หวังดีต่อบริษัท อันจะทำให้เป็นเป้าหมายในการสร้างความเสียหายให้เกิดขึ้นกับบริษัทรวมไปถึงเครือข่ายของโซ่อุปทานในที่สุด จุดมุ่งหมายของอาชญากรทางไซเบอร์ส่วนใหญ่มุ่งไปใน 3 ลักษณะคือ การนำความลับไปเปิดเผย (Data Confidentiality) การเปลี่ยนแปลงข้อมูล (Data Integrity) และการทำให้ระบบหยุดบริการหรือไม่สามารถใช้งานได้ (System Availability) (เศรษฐพงค์ มะลิสุวรรณ, 2010)

ผลของภัยคุกคามทางไซเบอร์อันเป็นมาจากการใช้งานอินเทอร์เน็ตในปัจจุบันนั้น เราจะเห็นได้ว่าภัยคุกคามไซเบอร์มีการพัฒนาและก้าวหน้ามากขึ้นเรื่อย ๆ เป็นภัยคุกคามที่ไม่เคยพบมาก่อน (Unknown Threats หรือ Zero-day Attacks) (TechTalkThai, 2016; Polatidis, N., 2017) เป็นสิ่งที่บริษัททั้งหลายทั้งในประเทศไทยและต่างประเทศทั่วโลกบริษัทกำลังเผชิญ เมื่อบริษัทเหล่านี้ได้รับการโจมตีจากภัยคุกคามที่ไม่รู้จักนี้ บริษัทเหล่านั้นต้องเผชิญกับความสูญเสียมหาศาล การโจมตีจากภัยคุกคามที่ไม่รู้จักเหล่านี้แทบจะหาวิธีการที่จะนำมาใช้ในการป้องกันไม่ได้เลย เนื่องจากการโจมตีเหล่านั้นเป็นสิ่งที่ไม่เคยพบเห็นมาก่อนเป็นการโจมตีที่สามารถเกิดขึ้นด้วยวิธีการใหม่ ๆ ได้อยู่ตลอดเวลา การหาวิธีการในการดำเนินการป้องกันไม่ว่าจะด้วยวิธีใดก็ไม่สามารถที่จะรับมือจากการโจมตีที่เกิดขึ้นเหล่านี้ได้ แต่หนึ่งในวิธีป้องกันที่ดีที่สุด คือวิธีการที่เกิดจากการเรียนรู้พฤติกรรมจากการใช้งาน (User Behavior Analytics หรือ Machine Learning) (TechTalkThai, 2016) โดยถ้าพบเห็นสิ่งที่ผิดปกติก็ให้ทำการแจ้งเตือนหรือกักกันสิ่งเหล่านั้นออกจากระบบ แต่อย่างไรก็ตาม วิธีดังกล่าวนี้ก็ไม่สามารถที่จะใช้ในการตรวจจับและป้องกัน ภัยคุกคามที่ไม่เคยพบมาก่อนนี้ได้ 100% หรือได้ทันก่อนที่การโจมตีเหล่านั้นจะทำอันตรายระบบของบริษัทลงได้

จากภาพประกอบที่ 1.3 แสดงให้เห็นว่า สำหรับประเทศไทยนั้นมีรายงานจาก Malware Infection Index (2016) ที่ได้ระบุว่าภูมิภาคเอเชียแปซิฟิกมีความเสี่ยงด้านมัลแวร์สูงกว่าภูมิภาคอื่น โดยจาก 5 อันดับแรกของประเทศที่เสี่ยงการติดมัลแวร์สูงสุด พบว่าเป็นชาติจากภูมิภาคนี้มีถึง 4 อันดับด้วยกัน สำหรับประเทศไทยเอง เสี่ยงสูงเป็นอันดับ 3 ในเอเชียแปซิฟิก และอันดับ 7 ของโลก นอกจากนั้นแล้ว รายงานจาก Security Intelligence Report (2016) ของไมโครซอฟท์ระบุว่าอัตราการตรวจพบมัลแวร์ในประเทศไทย ช่วงปลายปี 2558 เพิ่มสูงขึ้นถึง 6.9% เมื่อเทียบกับไตรมาสก่อนหน้า ขณะที่จำนวนเฉลี่ยของเครื่องคอมพิวเตอร์ที่ต้องกำจัดมัลแวร์ด้วยเครื่องมือของไมโครซอฟท์พุ่งสูงขึ้นจาก 22.2 เป็น 46.3 ต่อ 1,000 เครื่อง สถิติทั้งสองข้อนี้แสดงให้เห็นว่าประเทศไทยต้องเผชิญกับภัยร้ายในโลกดิจิทัลที่มีจำนวนเพิ่มมากขึ้นอย่างทวีคูณ ทั้งยังมีรูปแบบการ

จู่โจมที่ซับซ้อนมากขึ้น ความเปลี่ยนแปลงเหล่านี้ล้วนเป็นผลกระทบที่หลีกเลี่ยงไม่ได้ จากการพัฒนาสู่ยุคสังคมดิจิทัล



ภาพประกอบที่ 1.3 รายงานประเทศที่มีความเสี่ยงด้านมัลแวร์ประจำปี 2016

ที่มา : Malware Infection Index 2016 highlights key threats undermining cybersecurity in Asia Pacific: Microsoft Report

จากการสนับสนุนของภาครัฐโดยการประกาศนโยบายการขับเคลื่อนเศรษฐกิจดิจิทัล โดยคณะกรรมการเตรียมการด้านดิจิทัลเพื่อเศรษฐกิจและสังคม ได้เสนอแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และ แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย (พ.ศ.2559-2561) รวมถึงการพัฒนาศูนย์ข้อมูล (Data Center) และโครงการยกระดับโครงสร้างพื้นฐานโทรคมนาคมเพื่อขับเคลื่อนเศรษฐกิจมุ่งนำพาประเทศสู่ ดิจิทัลไทยแลนด์ (Digital Thailand) ทำให้หน่วยงานต่าง ๆ ทั้งภาครัฐและภาค

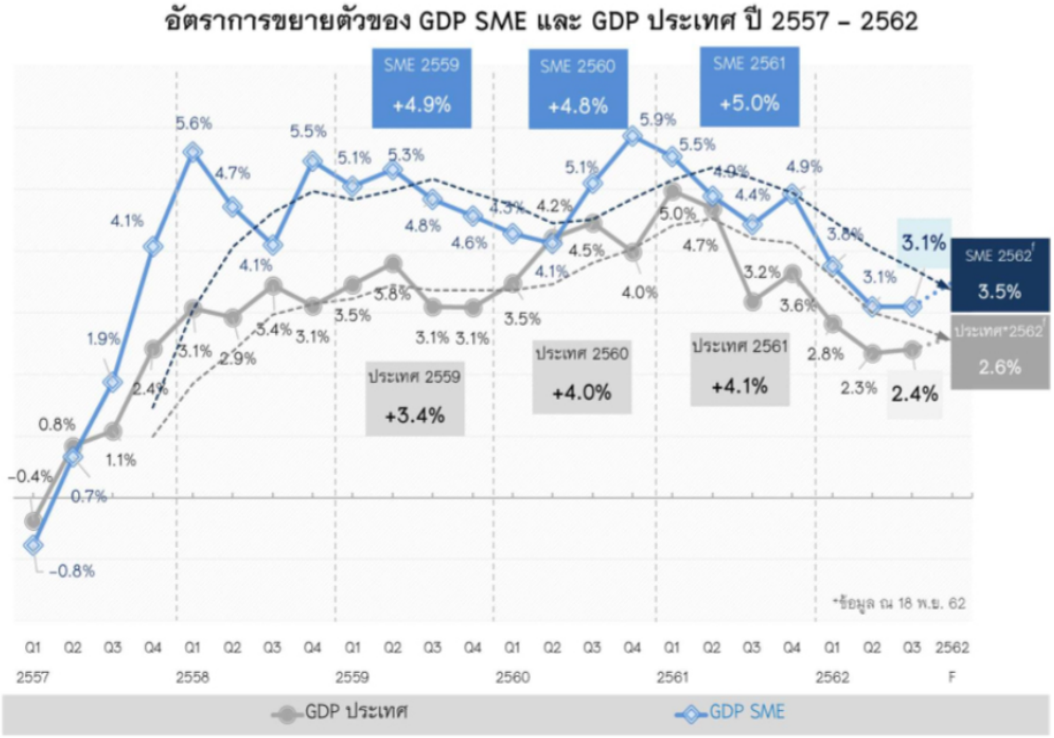
ธุรกิจของประเทศไทยเกิดความตื่นตัว ในการที่จะพัฒนาระบบการทำงานในแต่ละบริษัทเพื่อให้สามารถรองรับต่อนโยบายเศรษฐกิจดิจิทัลดังกล่าว เศรษฐกิจดิจิทัล (Digital Economy) เป็นระบบเศรษฐกิจที่ธุรกิจส่วนใหญ่ใช้เทคโนโลยีดิจิทัลทำการค้าการขาย ตั้งแต่การผลิต การสั่งซื้อ การส่งสินค้าตลอดจนการชำระเงิน ที่มีการดำเนินธุรกรรมมากกว่าการทำงานด้วยระบบคอมพิวเตอร์แบบเดิม เนื่องจากระบบธุรกิจถูกสร้างขึ้นจากความสัมพันธ์ระหว่างคนกับคน คนกับองค์กร และองค์กรกับองค์กรหรือกับกลุ่มองค์กร และกับสิ่งแวดล้อม สิ่งแวดล้อมในที่นี้อาจหมายถึง กฎหมาย กฎระเบียบของภาครัฐในบริบทของการทำธุรกิจ ชุมชน ลูกค้า คู่ค้า คู่แข่ง ระบบเครือข่ายคอมพิวเตอร์ ระบบงานอื่น ๆ ที่เกี่ยวข้องกับธุรกิจ รวมทั้งทรัพยากรขององค์กรที่เกี่ยวข้อง เช่นคน อุปกรณ์ สินค้า บริการ และทรัพยากรอื่น ๆ การอธิบายที่แสดงข้างต้น จึงเป็นการแสดงให้เห็นความสัมพันธ์ระหว่างองค์ประกอบที่กล่าวทั้งหมด และเชื่อมโยงกันผ่านดิจิทัลเทคโนโลยี จึงเรียกได้ว่าเป็น “ระบบนิเวศธุรกิจดิจิทัล (Digital Business Ecosystem)” และถือว่าเป็นเวทีการค้าที่สำคัญในยุคเศรษฐกิจดิจิทัล

อย่างไรก็ดี โมเดลประเทศไทย 4.0 (Thailand Economic 4.0) คือนโยบายพัฒนาเศรษฐกิจที่ปรับเปลี่ยนโครงสร้างการผลิต เน้นการใช้เทคโนโลยีและนวัตกรรมเพื่อเพิ่มมูลค่าสินค้าและบริการ เป็นนโยบายที่วางรากฐานการพัฒนาประเทศในระยะยาว โมเดลประเทศไทย 4.0 เป็นการพัฒนาแบบ “Value-Added Economy” ที่เน้นการสร้างมูลค่าเพิ่ม (แทนที่จะเป็นสินค้าแบบ Commodity) เน้นเทคโนโลยี (แทนที่จะเป็นอุตสาหกรรม) และเน้นการบริการ (มากกว่าขายสินค้า) เป้าหมายหลักของรัฐอยู่ที่ 5 อุตสาหกรรมที่ประเทศไทยมีองค์ความรู้ และศักยภาพที่จะพัฒนาต่อยอดได้ ได้แก่ กลุ่มอุตสาหกรรมอาหาร เกษตรและไบโอเทคโนโลยี (Food, Agriculture & Bio-tech) กลุ่มอุตสาหกรรมเพื่อสุขภาพ (Health , Wellness &Bio-Medical) กลุ่มอุตสาหกรรมอุปกรณ์อัจฉริยะและหุ่นยนต์เพื่ออุตสาหกรรม (Smart Devices Robotics & Mechatronics) กลุ่มอุตสาหกรรมดิจิทัล พัฒนาระบบการสื่อสาร และเทคโนโลยีสมัยใหม่ (Digital &Embedded Technology) และกลุ่มอุตสาหกรรมสร้างสรรค์และการเพิ่มมูลค่าการบริการ (Creative, Culture &High Value Service)

ในอนาคตการดำเนินการที่ในนโยบายสนับสนุนโมเดลประเทศไทย 4.0 จะเป็นรูปธรรมมากขึ้น ดังนั้นแล้ว การจัดการทางด้านโลจิสติกส์และโซ่อุปทาน ก็จะต้องเตรียมรับมือกับธุรกิจที่จะเติบโตไปในอนาคต แผนนโยบายที่ชัดเจนได้แก่ การพัฒนาการขนส่งชายแดน (Cross Border Logistics) การบริการส่งออก/นำเข้าสินค้า ตลอดจนการจัดการคลังสินค้า หรือต่อไปอาจจะกลายเป็น ศูนย์บริการลูกค้า (Fulfillment Center) โดยกลุ่มเป้าหมายที่ภาครัฐต้องการที่จะส่งเสริมก็คือ กลุ่มธุรกิจวิสาหกิจขนาดกลางและขนาดย่อมหรือเอสเอ็มอี การพัฒนาเอสเอ็มอีในปัจจุบันถือว่าเป็นวาระแห่งชาติเพราะว่าจำนวนเอสเอ็มอีในประเทศไทยมีมากถึงเกือบ 3 ล้านรายหรือร้อยละ

99.7 ของวิสาหกิจทั้งหมดนั้นเอง การสนับสนุนกลุ่มธุรกิจเอสเอ็มอีให้มีศักยภาพในการเข้าถึงตลาดที่ใหญ่ขึ้น และมีการเติบโตอย่างก้าวกระโดดให้ได้ตามเป้าหมายที่ตั้งไว้ นอกจากนี้ในการผลักดันโมเดลตามที่กล่าวมาแล้วนั้น ประเทศไทยจะต้องปฏิรูปโครงสร้างเศรษฐกิจจากเดิมที่เป็นการผลิตโดยใช้แรงงาน เครื่องจักรและทรัพยากร โดยจะต้องเปลี่ยนเป็นการผลิตบนฐานความรู้และเทคโนโลยี (Technology Base) การพัฒนาภาคบริการ รวมทั้งต้องมีการปฏิรูปการวิจัยและพัฒนาและการปฏิรูประบบการศึกษา ต้องเน้นไปที่การสร้างแรงงานที่มีความรู้เรื่องเทคโนโลยี เพื่อสอดคล้องกับแนวทางพัฒนาอุตสาหกรรมในอนาคต

จากรายงานสถานการณ์ของผู้ประกอบการเอสเอ็มอี ในปี 2562 (สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ, 2562) ตามภาพประกอบที่ 1.4 แสดงให้เห็นถึงโดยมูลค่าผลิตภัณฑ์มวลรวมภายในประเทศของวิสาหกิจขนาดกลางและขนาดย่อม (GDP SME) ของปี 2562 ขยายตัวได้ 3.1% มีมูลค่า 1.81 ล้านล้านบาท คิดเป็นสัดส่วน 43.6% ต่อ GDP รวมทั้งประเทศ และตารางที่ 1.2 โดยธุรกิจ SME ที่ขยายตัวได้ดีได้แก่ ธุรกิจบริการที่พักแรมและบริการด้านอาหาร ธุรกิจการเงินและการประกันภัย ธุรกิจด้านศิลปะความบันเทิงและนันทนาการ และบริการขนส่งและสถานที่เก็บสินค้า ธุรกิจ SME ที่ชะลอตัวลง ได้แก่ ธุรกิจก่อสร้าง ธุรกิจบริการด้านอสังหาริมทรัพย์



ภาพประกอบที่ 1.4 อัตราการขยายตัวของ GDP SME และ GDP ประเทศในปี 2557 - 2562

ที่มา : สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ

ตารางที่ 1.2 อัตราการขยายตัวของ GDP รายไตรมาสจำแนกตามสาขาธุรกิจ ปี 2560 - 2562

กิจกรรมทางเศรษฐกิจ	2560				2561				2562			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	9M62
การทำเหมืองแร่และเหมืองหิน	-7.8	-10.3	-7.6	-0.5	-1.5	2.1	-0.9	-0.2	-0.8	6.3	8.6	4.6
การผลิต	2.2	1.7	4.3	3.5	3.8	3.2	1.6	3.6	0.6	-0.2	-1.5	-0.3
ไฟฟ้า ก๊าซ ไอน้ำ และระบบปรับอากาศ	2.3	-1.1	3.8	3.8	2.5	1.8	1.2	5.0	5.4	7.3	1.9	4.9
การจัดหาน้ำ การจัดการและบำบัดน้ำเสีย	1.8	5.3	9.6	12.0	4.1	5.4	4.9	6.5	4.9	2.1	1.7	2.8
การก่อสร้าง	3.1	-6.3	-2.3	-5.9	1.2	1.9	4.5	3.4	3.0	3.4	2.7	3.0
การขายส่งและการขายปลีก การซ่อมยานยนต์ฯ	6.1	6.9	7.5	8.5	7.2	7.6	7.7	7.8	6.8	5.9	5.6	6.2
การขนส่งและสถานที่เก็บสินค้า	2.7	5.3	3.6	5.1	4.0	2.3	1.4	2.3	3.5	2.3	2.5	2.8
ที่พักแรมและบริการด้านอาหาร	7.2	9.8	9.6	16.7	13.3	9.0	4.2	5.5	4.9	3.7	6.6	5.0
ข้อมูลข่าวสารและการสื่อสาร	5.1	2.3	2.8	3.4	5.9	8.5	8.2	7.7	6.5	8.7	7.4	7.5
กิจกรรมทางการเงินและการประกันภัย	5.4	6.8	5.3	3.6	4.2	5.3	3.7	2.4	2.0	1.8	3.8	2.6
กิจกรรมอสังหาริมทรัพย์	4.8	6.6	7.1	7.5	6.0	4.0	5.9	4.9	4.7	3.1	2.6	3.5
กิจกรรมทางวิชาชีพ วิทยาศาสตร์ และเทคนิค	4.7	5.2	6.4	7.6	3.9	2.7	3.8	3.1	1.3	2.5	1.9	1.9
กิจกรรมการบริหารและการบริการสนับสนุน	1.4	3.9	3.3	5.8	5.7	3.8	1.5	2.1	-0.6	0.2	2.1	0.5
การศึกษา	-0.8	1.4	0.1	1.8	2.3	-0.1	-1.2	-0.7	1.2	1.6	1.3	1.3
กิจกรรมด้านสุขภาพและงานสังคมสงเคราะห์	3.6	4.1	4.2	2.9	4.8	4.3	2.3	4.3	3.5	3.9	3.7	3.7
ศิลปะ ความบันเทิง และนันทนาการ	11.5	9.6	9.8	17.4	10.8	8.2	14.0	12.2	11.6	9.8	11.0	10.8
กิจกรรมบริการด้านอื่นๆ	5.2	5.1	4.8	2.6	3.2	2.8	4.8	4.3	2.5	2.3	1.8	2.2
กิจกรรมการจ้างงานในครัวเรือนส่วนบุคคล	-0.4	-0.9	-4.9	-1.7	-0.9	-2.6	-3.8	-3.3	-0.1	-0.7	2.4	0.5
รวม	4.3	4.1	5.1	5.9	5.5	4.9	4.4	4.9	3.8	3.1	3.1	3.3

ที่มา : สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ

และธุรกิจบริการทางวิชาชีพฯ ธุรกิจ SME ที่หดตัวได้แก่ ภาคการผลิต โดยหดตัวลงถึง 1.5% อันเป็นผลมาจากการ หดตัวของอุตสาหกรรมวัตถุดิบ เช่น การพิมพ์ ยางและพลาสติก และอุตสาหกรรมสินค้าทุนและเทคโนโลยี เช่น เครื่องจักร คอมพิวเตอร์และอุปกรณ์ ซึ่งส่วนหนึ่งมาจากการหดตัวของภาคการส่งออก และแผนแม่บทส่งเสริมผู้ประกอบการวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) ฉบับที่ 4 เพื่อประกาศใช้ในปี 2560-2564 โดยเน้นการเพิ่มสัดส่วนผลิตภัณฑ์มวลรวมภายในประเทศ (GDP) ของวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) และให้วิสาหกิจขนาดกลางและขนาดย่อม (SMEs) เป็นภาคส่วนที่ขับเคลื่อนไทยสู่การเป็นกลุ่มประเทศรายได้สูง ด้วยเหตุนี้เองการสนับสนุนส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อมจากทางภาครัฐภายใต้นโยบายโมเดลประเทศไทย 4.0 เพื่อต้องการให้วิสาหกิจขนาดกลางและขนาดย่อม (SMEs) ทำหน้าที่ในการขับเคลื่อนเศรษฐกิจของประเทศ

ถึงแม้ว่าความเสี่ยงทางไซเบอร์ โดยเฉพาะการโจมตีทางไซเบอร์ที่มีต่อองค์กรหรือบริษัทต่าง ๆ นั้นจะอยู่ในช่วงเริ่มแรก แต่การโจมตีเหล่านี้ได้เกิดขึ้นมานานหลายปีแล้วเพียงแต่อาจจะไม่มีความรุนแรงเท่าในปัจจุบัน และด้วยจำนวนการโจมตีที่เพิ่มขึ้น อันเป็นผลมาจากการขาดความพร้อมซึ่งเป็นปัญหาสำคัญที่จำเป็นต้องได้รับการจัดการดูแลอย่างจริงจัง ประเด็นที่องค์กรหรือบริษัทต่าง ๆ ต้องตั้งคำถามก็คือว่า องค์กรหรือบริษัทได้มีการดำเนินการอย่างเพียงพอแล้วหรือยังเพื่อที่จะปกป้องธุรกิจของตัวเองจากภัยคุกคามทางไซเบอร์ องค์กรหรือบริษัทต่าง ๆ จำเป็นที่

จะต้องทำการปรับปรุงระบบเพื่อป้องกันภัยคุกคามในรูปแบบใหม่ได้แล้วหรือไม่ ดังนั้นแล้วไม่เพียงแต่ที่จะต้องระวังต่อภัยคุกคามในรูปแบบใหม่ที่เข้ามา หากแต่จะต้องระวังต่อภัยคุกคามในรูปเดิมด้วยเช่นกัน และจำเป็นที่จะต้องทำโดยให้ครอบคลุมทุกระบบและทุกกลุ่มอุตสาหกรรมอย่างไม่มีข้อยกเว้น

ความปลอดภัยของไซเบอร์ใน SMEs นั้นเพิ่มขึ้นอย่างต่อเนื่องเนื่องจากการใช้เทคโนโลยีดิจิทัลที่เพิ่มขึ้น อย่างเช่นการประมวลผลแบบคลาดว์ (Cloud Computing) และอินเทอร์เน็ตประสานสรรพสิ่ง (Internet of Things (IoT)) ซึ่งยังรวมไปถึงอุปกรณ์ดิจิทัลที่หลากหลายที่มีการเชื่อมต่ออินเทอร์เน็ตได้เพื่อทำให้เกิดธุรกรรมทางด้านธุรกิจ ไม่ว่าจะเป็น คอมพิวเตอร์ส่วนบุคคล คอมพิวเตอร์แม่ข่าย อุปกรณ์พกพา อุปกรณ์ส่วนตัวที่นำมาใช้ในที่ทำงาน การเข้าถึงจากระยะไกล การใช้โปรแกรมสำเร็จรูปและบริการบนคลาวด์ โดยการเชื่อมต่อที่เพิ่มขึ้นจะมาพร้อมกับเทคโนโลยีอินเทอร์เน็ตซึ่งทำให้เกิดพื้นที่ที่ใหญ่ขึ้นสำหรับการโจมตีจากฝ่ายตรงข้าม ด้วยการใช้ประโยชน์จากช่องว่างด้านความปลอดภัยของอุปกรณ์ที่มีการเชื่อมต่ออินเทอร์เน็ต ด้านหนึ่งการที่องค์กรมีโปรโตคอลที่ปลอดภัยสามารถปกป้องข้อมูลองค์กรจากการถูกดักข้อมูลรวมทั้งจากการเข้าถึงระบบของบริษัทโดยไม่ได้รับอนุญาต หรือแม้แต่การปฏิเสธการโจมตีบริการและยังจะสามารถช่วยให้บริษัทปลอดภัยจากการละเมิดที่อาจมีค่าใช้จ่ายมากตามมา ในทางตรงกันข้ามความมั่นคงปลอดภัยมีผลให้เกิดการสื่อสารที่ลดลง จึงเป็นสิ่งสำคัญที่จะต้องปรับความสมดุลให้เหมาะสมระหว่างการรักษาความมั่นคงปลอดภัยและการสื่อสารให้มีประสิทธิภาพ ดังนั้นจึงมีความจำเป็นที่จะต้องมีกลไกในการรักษาความมั่นคงปลอดภัยที่สามารถตรวจจับการโจมตีไม่เพียง แต่ในระดับเครือข่าย แต่ยังต้องอยู่ในระดับชั้นของแอพลิเคชัน รวมไปถึงการระวังและป้องกันต่อช่องโหว่ที่อาจจะเกิดขึ้นจากโปรโตคอลต่าง ๆ ได้

จากรายงานภัยคุกคามด้านความมั่นคงปลอดภัยบนอินเทอร์เน็ต (Internet Security Threat Report หรือ ISTR) ฉบับที่ 20 ของไซแมนเทค (Nasdaq: SYMC) เปิดเผยว่า บริษัทต่าง ๆ ทุกบริษัทไม่ว่าจะมีขนาดเล็กหรือขนาดใหญ่ ล้วนตกเป็นเป้าหมายการโจมตีทางไซเบอร์ได้ทั้งสิ้น สำหรับในประเทศไทยบริษัทที่ดำเนินธุรกิจขนาดกลางและขนาดย่อม (SMEs) มีพนักงานน้อยกว่า 500 คน ประมาณ 9 ใน 10 แห่งตกเป็นเป้าหมายการโจมตีแบบ ฟิชชิ่งที่มีเป้าหมายชัดเจนหรือสเปียร์ฟิชชิ่ง (Spear-phishing) ขณะที่การโจมตีเหล่านี้มีลักษณะซับซ้อนมากขึ้น ระบบรักษาความมั่นคงปลอดภัยทางด้านไอทีจึงมีความจำเป็น และควรปรับใช้แนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างกว้างขวาง

นอกจากนี้ยังมีการศึกษาของ Finnerty, K. et al. (2018) ที่แสดงให้เห็นว่าธุรกิจขนาดกลางและขนาดย่อมต้องประสบปัญหาการโจมตีทางไซเบอร์ในระดับสูง อีกยังในรายงานยังแสดงให้

เห็นว่าธุรกิจขนาดกลางและขนาดย่อมจะมีช่องว่างในการรับรู้ถึงภัยคุกคามทางไซเบอร์ ในเรื่องของการตระหนักถึงการเตรียมความพร้อมต่อภัยคุกคามดังกล่าว ในทำนองเดียวกันตาม FireEye (2016) ที่ระบุว่า 77% ของอาชญากรรมไซเบอร์ทั้งหมดที่เกิดขึ้นมีเป้าหมายการโจมตีไปที่ SMEs การป้องกันการโจมตีดังกล่าวด้วยโปรแกรมป้องกันไวรัสที่ SMEs ใช้อยู่นั้นไม่เพียงพอแล้วสำหรับการโจมตีทางไซเบอร์ในปัจจุบัน เนื่องจากความซับซ้อนและความหลากหลายของภัยคุกคามทางไซเบอร์ การบูรณาการเทคโนโลยีดิจิทัลได้เกิดขึ้นอย่างมากมายในกระบวนการทางธุรกิจ ที่ทำให้เกิดมูลค่าทางเศรษฐกิจเป็นอย่างมาก แม้ในองค์กรขนาดเล็กที่สุดก็ตาม

ดังที่ได้กล่าวไว้ถึงกรณีของภัยคุกคามที่เกิดขึ้น อันเนื่องจากการโจมตีทางไซเบอร์และอาชญากรรมทางไซเบอร์ดังที่ได้กล่าวมาแล้วนั้น เป็นประเด็นได้ที่ได้รับความสนใจอย่างมากมายและกว้างขวางอย่างมากในภาคธุรกิจ แต่ก็ยังเป็นเรื่องที่ได้ความสนใจจากกลุ่มนักวิชาการอยู่น้อยมาก เหตุผลหนึ่งที่กลุ่มนักวิชาการไม่ค่อยได้ให้ความสนใจในเรื่องของภัยคุกคามทางไซเบอร์ที่เกิดจากความเสี่ยงที่ไม่รู้จัก เป็นผลอันเนื่องมาจากการที่ต้องนำเอาองค์ความรู้จากสองสาขาที่มีแตกต่างกันมาบูรณาการร่วมกัน ได้แก่ เทคโนโลยีสารสนเทศ/ดิจิทัล และโลจิสติกส์และโซ่อุปทาน โดยการศึกษาที่ผ่านมาได้มีการศึกษาระบบเทคโนโลยีสารสนเทศกับโซ่อุปทาน แต่ในมุมมองที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ได้แก่ ความเสี่ยงทางไซเบอร์ ภัยคุกคามทางไซเบอร์ จุดอ่อนหรือช่องโหว่ ผลกระทบทางไซเบอร์ และโอกาสที่จะเกิดขึ้นของเหตุการณ์ทางไซเบอร์ เป็นต้น จะยังไม่มีนักวิชาการได้กล่าวถึงมากนัก โดยเฉพาะในเรื่องการคืนสภาพได้ทางด้านไซเบอร์ในโซ่อุปทานดิจิทัล เราจะเห็นได้ในปัจจุบันว่าระบบโซ่อุปทานดิจิทัล ในปัจจุบันจะต้องเผชิญกับความเสี่ยงทางไซเบอร์ดังกล่าวนี้เป็นความปกติแบบใหม่ (New Normal) ในทุก ๆ วัน ผลกระทบทางไซเบอร์นับวันจะยิ่งรุนแรงมากขึ้นอันเป็นภัยพิบัติทางไซเบอร์ที่มีผลต่อการล่มสลายขององค์กรธุรกิจและความเชื่อมั่นของลูกค้า ทั้งนี้การที่องค์กรมีความทนทานคล่องตัว และมีความสามารถที่จะดำเนินงานต่อไปได้ แม้จะประสบปัญหาจากภัยคุกคามที่คาดไม่ถึงทางไซเบอร์ รวมทั้งมีแนวทางในการเตรียมความพร้อมขององค์กรให้สามารถป้องกัน ต่อต้าน ตรวจจับและตอบสนองต่อการบุกรุก การจารกรรม หรือการหลอกลวงที่จะทำให้องค์กรเสียหายได้ ในที่นี้จะเรียกว่า การคืนสภาพได้ทางไซเบอร์ ดังนั้น การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลจะสามารถหลีกเลี่ยง ลดความเสี่ยงทางไซเบอร์ และดำรงไว้ซึ่งการดำเนินงานที่ต่อเนื่องและยั่งยืนขององค์กรธุรกิจ

ผู้วิจัยมีความสนใจว่า ธุรกิจเอสเอ็มอีที่ใช้ระบบโซ่อุปทานดิจิทัลหรือเอสเอ็มอีดิจิทัลของเราต้องเผชิญกับภัยคุกคามทั้งในรูปแบบเดิมและรูปแบบใหม่ ภัยคุกคามรูปแบบใหม่ที่เกิดขึ้นอาทิ ความเสี่ยงทางไซเบอร์ ภัยคุกคามทางไซเบอร์ การระบุและวิเคราะห์ภัยคุกคามที่ชัดเจนดังเช่น

ในอดีตทำได้ยาก ดังนั้น จึงต้องหาวิธีใหม่ในแการแก้ไขปัญหาด้วยความรวดเร็ว รอบคอบ และใช้ทักษะความรู้ ความเชี่ยวชาญขั้นสูงในการปฏิบัติ อนึ่ง การเพิ่มขึ้นของความเสี่ยงทางไซเบอร์ที่เกิดมาจากภัยคุกคามทางไซเบอร์นี้ส่วนหนึ่งเป็นผลมาจากการขาดความรู้ความเข้าใจ ความตระหนักรู้ ขาดวุฒิภาวะความสามารถทางไซเบอร์ ขาดการรับมือและฟื้นสภาพทางไซเบอร์ได้อย่างทันท่วงที รวมทั้งขาดความพร้อมทางไซเบอร์ในระบบโซ่อุปทานดิจิทัล ปัญหาเหล่านี้มีความสำคัญเป็น อย่างยิ่ง จำเป็นต้องได้รับการจัดการดูแลอย่างจริงจังและต่อเนื่อง ประเด็นที่เราต้องตั้งคำถามก็คือว่า เราได้ดำเนินการอย่างเพียงพอแล้วหรือยังเพื่อที่จะปกป้องธุรกิจของตัวเราเองจากภัยคุกคามทางไซเบอร์ เราจำเป็นที่จะต้องปรับปรุงระบบเพื่อป้องกันภัยคุกคามรูปแบบใหม่ ดังนั้นแล้วไม่เพียงแต่ที่จะต้องระวังต่อภัยคุกคามรูปแบบใหม่ ที่เข้ามา แต่จะต้องระวังต่อภัยคุกคามรูปแบบเดิมด้วยเช่นกัน ในรอบหลายสิบปีที่ผ่านมาธุรกิจขนาดกลางและขนาดใหญ่ในประเทศไทยต่างได้ลงทุนด้านไอซีทีไปค่อนข้างมาก และได้สร้างสมรรถนะในการแข่งขันด้วยไอซีที การทำธุรกิจออนไลน์และแลกเปลี่ยนข้อมูลทางการค้ากับพันธมิตรด้วยเอกสารอิเล็กทรอนิกส์ก็ได้พัฒนาไปแล้วไม่แพ้ประเทศอื่น ทั้งนี้จะต่างกับธุรกิจกลุ่มวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) ที่ส่วนใหญ่ยังไม่ได้พัฒนาระบบธุรกิจไปในทิศทางที่กล่าวข้างต้นเป็นเรื่องปกติของธุรกิจวิสาหกิจขนาดกลางและขนาดย่อมทั่วทั้งโลกที่เป็นกลุ่มที่ใช้ไอซีทีน้อยที่สุดด้วยเหตุผลที่พอเข้าใจได้ จึงจำเป็นที่ภาครัฐต้องเข้ามาส่งเสริมธุรกิจกลุ่มนี้ให้เข้าสู่การใช้ระบบออนไลน์ด้วยเอกสารอิเล็กทรอนิกส์ให้มากที่สุด เพื่อยกระดับความสามารถการแข่งขันทั่วทั้งระบบเศรษฐกิจของไทยในที่สุด

1.2 คำถามการวิจัย

เมื่อได้ศึกษาถึงทฤษฎี แนวคิด และงานวิจัยที่เกี่ยวข้องกับการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และตัวแบบวุฒิภาวะความสามารถในแง่มุมต่าง ๆ เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัลแล้วนั้น ผู้วิจัยได้พบประเด็นปลายเปิดจนนำไป สู่ข้อสังเกตและข้อคำถามในการวิจัย ดังนี้

1. การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล เป็นอย่างไร
2. ปัจจัยอะไรบ้าง ที่ส่งผลต่อความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล
3. ตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ควรเป็นอย่างไร

4. ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ควรเป็นอย่างไร
5. การประเมินตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลกับการจัดการความต่อเนื่องทางธุรกิจดิจิทัลนั้น จะสามารถทำได้อย่างไร

1.3 วัตถุประสงค์ของการวิจัย

ในการวิจัยครั้งนี้ ผู้วิจัยมีวัตถุประสงค์หลักของการวิจัยดังต่อไปนี้

1.3.1 เพื่อศึกษาถึงอิทธิพลของปัจจัยที่มีผลต่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และอิทธิพลของการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลที่มีผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

1.3.2 เพื่อพัฒนาตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

1.3.3 เพื่อพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

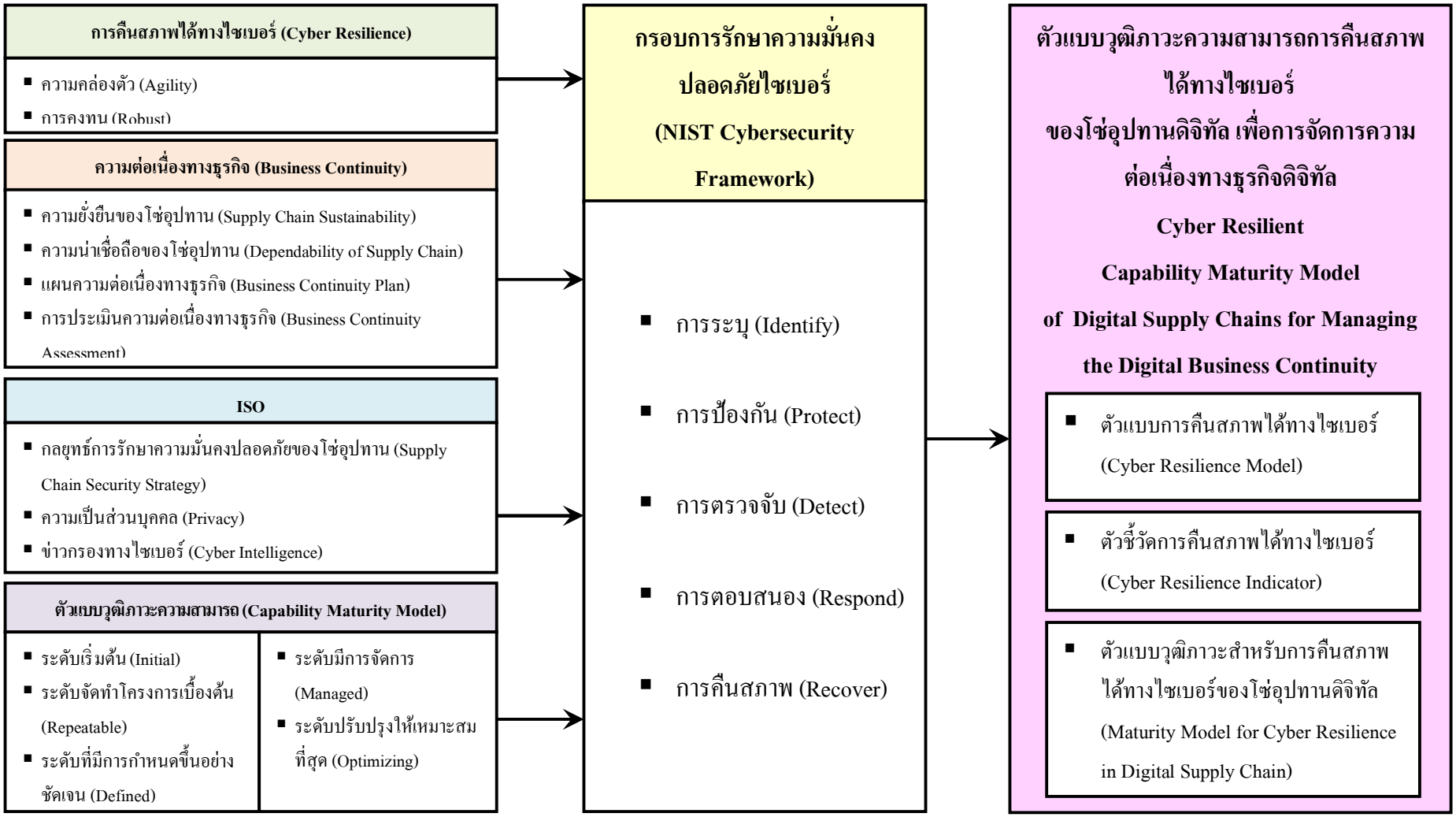
1.3.4 เพื่อทำการประเมินตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

1.3.5 เพื่อทำการพัฒนาระบบการประเมินระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

1.4 กรอบแนวคิดการวิจัย

งานวิจัยเรื่อง “การพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม” เพื่อให้ได้มาซึ่งตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ผู้วิจัยได้ทำการศึกษาถึงองค์ประกอบต่าง ๆ เพื่อที่จะได้นำมาใช้สำหรับการพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล โดยกรอบแนวคิดพื้นฐานในการศึกษาจะเกี่ยวข้องกับ (1) ปัจจัยที่ส่งผลและผลของการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ผู้วิจัยใช้แนวคิดจากงานวิจัยของ Wieland and Wallenburg (2013) ประกอบด้วย ความคล่องตัวและความคงทน โดยปัจจัยที่ส่งผลต่อความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ประกอบด้วยปัจจัยด้านความ

ร่วมมือกันของโซ่อุปทานดิจิทัล ผู้วิจัยใช้แนวคิดจากงานวิจัยของ Barratt (2004) Cao et al. (2010) และ Scholten (2015) ประกอบด้วย การแบ่งปันข้อมูลร่วมกัน ความไว้ใจ ความร่วมมือกันในการสื่อสาร และการสร้างความรู้ร่วมกัน ปัจจัยด้านการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล ผู้วิจัยใช้แนวคิดจากงานวิจัยของ Samuel Waithaka (2016) และ Srisawang and Sirirat (2015) ประกอบด้วย แรงจูงใจการโจมตีจากภายนอก ช่องโหว่การดำเนินการภายใน และการรับมือต่อภัยคุกคาม และปัจจัยด้านการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล ผู้วิจัยใช้แนวคิดจากงานวิจัยของ Dave Shackleford (2015) ประกอบด้วย บุคลากร กระบวนการ และเทคโนโลยี โดยผลของการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ได้แก่การจัดการความต่อเนื่องทางธุรกิจดิจิทัล ซึ่ง ผู้วิจัยได้นำแนวคิดจากมาตรฐานการจัดการความต่อเนื่องทางธุรกิจ (ISO 22301) ที่ประกอบด้วย แผนความต่อเนื่องทางธุรกิจ แผนการกู้คืนภัยพิบัติ การจัดการวิกฤตและการจัดการเหตุฉุกเฉิน มาเป็นแนวคิดสำหรับการศึกษาวิจัย (2) องค์ประกอบที่จะนำมาใช้ในการพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล โดยมีแนวพื้นฐานเพิ่มเติมประกอบด้วย แนวคิดด้านการจัดการความต่อเนื่องทางธุรกิจ ได้แก่ ความยั่งยืนของโซ่อุปทาน ความน่าเชื่อถือของโซ่อุปทาน แผนการจัดการความต่อเนื่องทางธุรกิจ และการประเมินความต่อเนื่องทางธุรกิจ ที่มาจากการนำเอาแนวคิดมาจากมาตรฐานการจัดการความต่อเนื่องทางธุรกิจ (ISO 22301) มาใช้ แนวคิดด้านมาตรฐานที่เกี่ยวข้องกับ กลยุทธ์การรักษาความมั่นคงปลอดภัยของโซ่อุปทาน ที่ได้นำเอาแนวคิดมาจากมาตรฐานการรักษาความมั่นคงปลอดภัยของโซ่อุปทาน (ISO 28000) แนวคิดความเป็นส่วนบุคคล ที่ได้แนวคิดมาจาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แนวคิดข่าวกรองทางไซเบอร์ ที่นำเอาแนวคิดมาจาก กระทรวงกลาโหมของสหรัฐอเมริกา รวมทั้งยังได้นำเอาแนวคิดของตัวแบบวุฒิภาวะความสามารถที่พัฒนาโดย Software Engineering Institute (SEI) ของมหาวิทยาลัยคาร์เนกี เมลลอน (Carnegie Mellon University) ที่ได้นำเสนอแนวคิดของระดับวุฒิภาวะความสามารถไว้ 5 ระดับได้แก่ ระดับเริ่มต้น (Initial Level) ระดับจัดทำโครงการเบื้องต้น (Repeatable) ระดับที่มีการกำหนดขึ้นอย่างชัดเจน (Defined) ระดับมีการจัดการ (Managed) ระดับปรับปรุงให้เหมาะสมที่สุด (Optimizing) (3) กรอบอ้างอิงในการพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการพัฒนาความต่อเนื่องทางธุรกิจดิจิทัล โดยผู้วิจัยได้ใช้แนวคิดมาจากกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework) ที่ประกอบด้วย การระบุ (Identify) การป้องกัน (Protect) การตรวจจับ (Detect) การตอบสนอง (Respond) และการคืนสภาพ (Recover) โดยกรอบแนวคิดในการวิจัยทั้งหมดได้แสดงไว้ดังภาพประกอบที่ 1.5



ภาพประกอบที่ 1.5 กรอบแนวคิดในการวิจัย

1.5 สมมติฐานการวิจัย

การวิจัยในเรื่อง “การพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม” ผู้วิจัยได้ทำการกำหนดสมมติฐานการวิจัย ดังนี้

1.5.1 ความร่วมมือกันของโซ่อุปทานดิจิทัล มีอิทธิพลทางบวกต่อความสามารถสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

1.5.2 การจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัลมีอิทธิพลทางบวกต่อความสามารถสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

1.5.3 การจัดการความเสี่ยงของโซ่อุปทานดิจิทัลมีอิทธิพลทางบวกต่อความสามารถสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล

1.5.4 ความร่วมมือกันของโซ่อุปทานดิจิทัล มีอิทธิพลทางบวกต่อการจัดการความเสี่ยงของโซ่อุปทานดิจิทัล

1.5.5 การจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล มีอิทธิพลทางบวกต่อการจัดการความเสี่ยงของโซ่อุปทานดิจิทัล

1.5.6 ความสามารถสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลมีอิทธิพลทางบวกต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

1.5.7 ตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล มีระดับความเหมาะสมอยู่ในระดับมาก

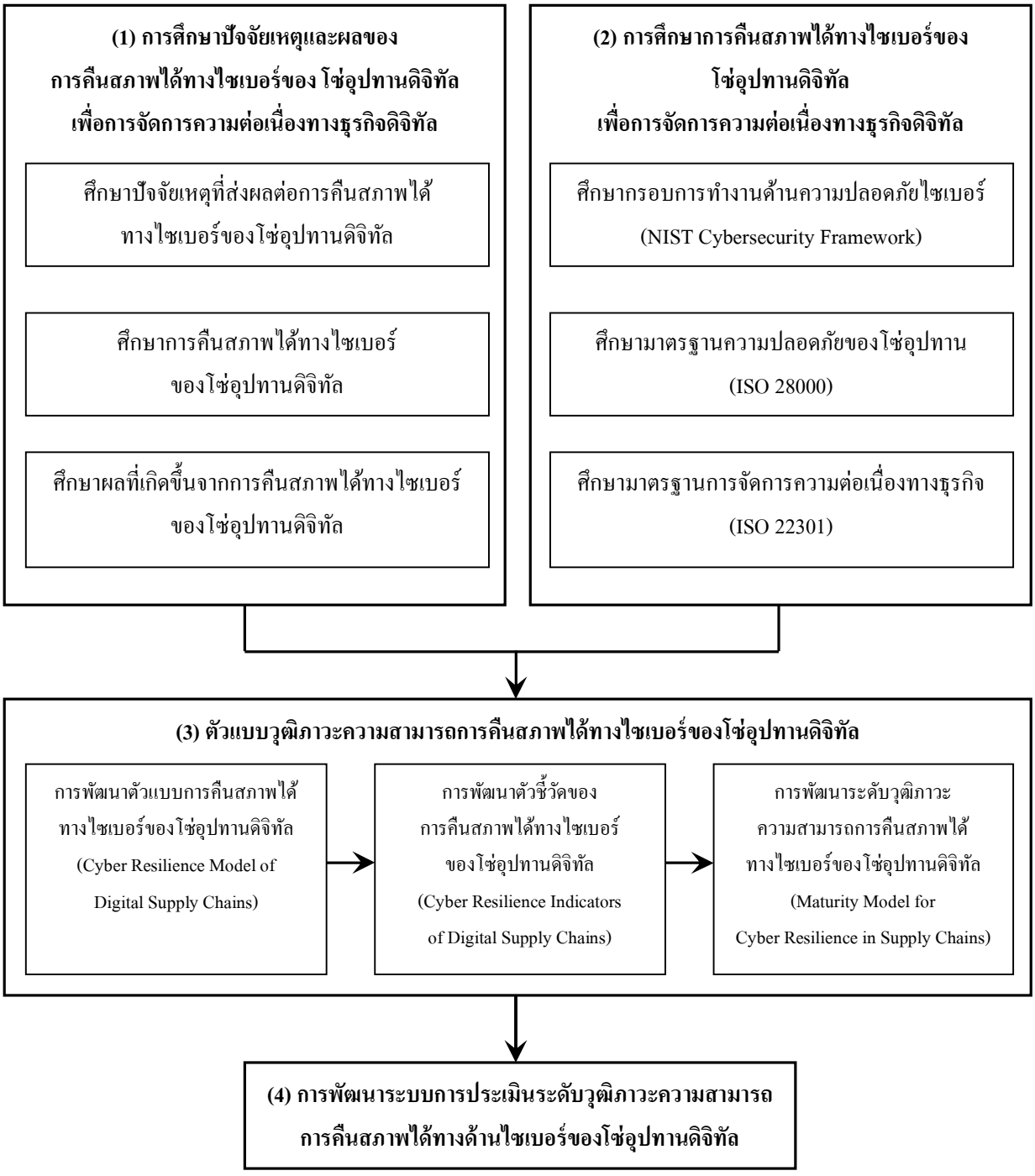
1.5.8 ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล มีระดับการยอมรับอยู่ในระดับมาก

1.6 ขอบเขตการวิจัย

การวิจัยเรื่อง “การพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม” ผู้วิจัยได้กำหนดขอบเขตของการวิจัย ดังนี้

1. ขอบเขตด้านเนื้อหา

การวิจัยครั้งนี้ ผู้วิจัยมุ่งเน้นศึกษา เพื่อการพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม โดยผู้วิจัยมีการกำหนดขอบเขตด้านเนื้อหาซึ่งแบ่งได้เป็น 4 องค์ประกอบ ดังแสดงได้ตามภาพประกอบที่ 1.6



ภาพประกอบที่ 1.6 ขอบเขตการวิจัยด้านเนื้อหา

องค์ประกอบที่ 1: **การศึกษาปัจจัยเหตุและผลของความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล** องค์ประกอบในส่วนนี้จะเป็นการศึกษาถึงปัจจัยเหตุและผลของความสามารถการคืนสภาพได้ทางไซเบอร์ของ

โซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล โดยผู้วิจัยได้ทำการทบทวนวรรณกรรมงานวิจัยของต่างประเทศและในประเทศ เพื่อนำมาพัฒนาเป็นกรอบแนวคิด พื้นฐานในการศึกษาเกี่ยวกับปัจจัยเหตุและผลของความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ได้แก่ (1) ด้านความร่วมมือกันของโซ่อุปทานดิจิทัล ผู้วิจัยใช้แนวคิดจากงานวิจัยของ Barratt (2004) Cao et al. (2010) และ Scholten (2015) ประกอบด้วย การแบ่งปันข้อมูลร่วมกัน ความไว้ใจ ความร่วมมือกันในการสื่อสาร และการสร้างความรู้ร่วมกัน (2) ด้านการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล ผู้วิจัยใช้แนวคิดจากงานวิจัยของ Samuel Waithaka (2016) และ Srisawang and Sirirat (2015) ประกอบด้วย แรงจูงใจการโจมตีจากภายนอก ช่องโหว่การดำเนินการภายใน และการรับมือต่อภัยคุกคาม (3) ด้านการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล ผู้วิจัยใช้แนวคิดจากงานวิจัยของ Dave Shackleford (2015) ประกอบด้วย บุคลากร กระบวนการ และเทคโนโลยี (4) ความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ผู้วิจัยใช้แนวคิดจากงานวิจัยของ Wieland and Wallenburg (2013) ประกอบด้วย ความคล่องตัวและความคงทน และ (5) ด้านการจัดการความต่อเนื่องทางธุรกิจ ผู้วิจัยได้นำแนวคิดจากมาตรฐานการจัดการความต่อเนื่องทางธุรกิจ (ISO 22301) ที่ประกอบด้วย แผนความต่อเนื่องทางธุรกิจ แผนการกู้คืนภัยพิบัติ การจัดการวิกฤต และการจัดการเหตุฉุกเฉิน

องค์ประกอบที่ 2: การศึกษาการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล องค์ประกอบในส่วนนี้จะเป็นการศึกษาถึงหลักการที่จะนำมาใช้ในการพัฒนาตัวแบบ และตัวชี้วัดความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล ที่เหมาะสมกับบริบทของวิสาหกิจขนาดกลางและขนาดย่อมของประเทศไทย ซึ่งจะได้มาจากการค้นคว้าเอกสารและงานวิจัยที่เกี่ยวข้อง รวมถึงศึกษากรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์จากองค์กร หน่วยงานต่าง ๆ ทั้งในและต่างประเทศ โดยผลที่ได้จากการพัฒนาในส่วนนี้จะทำการเชื่อมโยงกับมาตรฐานกรอบแนวคิดที่ได้รับการยอมรับในระดับสากล ที่ประกอบไปด้วย กรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework) มาตรฐานความมั่นคงปลอดภัยของโซ่อุปทาน (ISO 28000) มาตรฐานการจัดการความต่อเนื่องทางธุรกิจ (ISO 22301) โดยจะนำมารวมกับผลที่ได้จากการดำเนินการในองค์ประกอบที่ 1 เพื่อหาความสัมพันธ์เชื่อมโยง และนำไปสู่การพัฒนาเป็นตัวแบบและตัวชี้วัดความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัลต่อไป

องค์ประกอบที่ 3: ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล องค์ประกอบในส่วนนี้ จะเป็นการนำเอาผลจากการศึกษาในองค์ประกอบที่ 2 มา

ทำการ 1) พัฒนาตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Model) 2) พัฒนาตัวชี้วัดของการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Indicators) และ 3) พัฒนาระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Maturity Model for Cyber Resilience Supply Chains) เพื่อให้ได้เป็นตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และจะได้ดำเนินการให้มีการตรวจสอบความสอดคล้องของตัวแบบที่ได้โดยการประเมินจากกลุ่มผู้เชี่ยวชาญทางด้านโลจิสติกส์และโซ่อุปทาน ผู้เชี่ยวชาญด้านตัวแบบวุฒิภาวะความสามารถ (Capability Maturity Model : CMM) ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) และผู้เชี่ยวชาญด้านเทคโนโลยีดิจิทัล (Digital Technology) เพื่อให้ได้รับผลยืนยันที่เกี่ยวกับระดับความเหมาะสมและระดับการยอมรับและความสัมพันธ์ที่เกิดขึ้น

องค์ประกอบที่ 4 : การพัฒนาระบบการประเมินระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล องค์ประกอบในส่วนนี้จะเป็นการพัฒนาระบบสารสนเทศตามองค์ความรู้ที่ได้รับจากองค์ประกอบที่ 3 ตามกรอบแนวคิดของตัวแบบและตัวชี้วัดในแต่ละองค์ประกอบ โดยจะพัฒนาเป็นระบบในลักษณะของโปรแกรมประยุกต์ด้วยมาโคร บนไมโครซอฟท์ เอ็กซ์เซล เพื่อก่อให้เกิดความสะดวกในการประเมิน รวมถึงสามารถวิเคราะห์ช่องว่าง (Gap Analysis) ในตัวชี้วัดแต่ละตัว เพื่อให้ผู้บริหารได้เห็นถึงช่องว่าง จุดแข็งและจุดที่ควรพัฒนาของความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล รวมถึงจะได้เห็นมิติในการระบุ ป้องกัน ตรวจสอบ ตอบสอง การกู้คืน และความต่อเนื่อง ของธุรกิจรวมไปถึงโซ่อุปทานดิจิทัล นอกจากนี้ระบบยังให้คำแนะนำสำหรับตัวชี้วัดที่ยังเป็นจุดที่ควรพัฒนาแก่ผู้บริหาร เพื่อเป็นแนวทางในการปรับปรุงความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ได้อย่างมีทิศทาง มีเป้าหมาย และมีประสิทธิภาพ

2. ขอบเขตด้านประชากรและกลุ่มตัวอย่าง

ประชากรในการศึกษาครั้งนี้ คือ วิสาหกิจขนาดกลางและขนาดย่อม (Small Medium Enterprises : SMEs) โดยผู้วิจัยได้เลือก SMEs โดยแบ่งตามภาคธุรกิจได้แก่ ภาคการค้า ภาคการบริการ ภาคการผลิต และภาคธุรกิจการเกษตร เนื่องจากผู้วิจัยต้องการธุรกิจที่มีความเกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ที่มีการใช้งานทางอินเทอร์เน็ตรวมถึงการใช้โปรแกรมสำเร็จรูปในการบริหารงานภายในเป็นสำคัญ ซึ่งจะมีผลดีต่อการวิจัยในการที่จะให้ผลการวิจัยที่มีความชัดเจน โดยกลุ่มตัวอย่าง ผู้วิจัยใช้วิธีการกำหนดกลุ่มตัวอย่างตามกฎแห่งความชัดเจน (Rule of Thump) ตามข้อเสนอของ Schumacker & Lomax. (1996), Hair, Anderson, Tatham & Black. (1998) ที่นักสถิติวิเคราะห์ตัวแปรพหุนิยมใช้ คือ ใช้ขนาดกลุ่มตัวอย่าง 10 - 20 คน ต่อตัวแปรในการวิจัยหนึ่ง

ตัวแปร (Schumacker & Lomax, 1996., Hair et al., 1998 อ้างใน นงลักษณ์ วิรัชชัย, 2542) จากนั้นได้กำหนดขนาดตัวอย่างแยกตามสัดส่วนของภาคธุรกิจ เพื่อให้ได้ตัวอย่างครบตามในทุกภาคธุรกิจของ SMEs ต่อไป

3. ขอบเขตด้านเวลา

การวิจัยครั้งนี้ ผู้วิจัยดำเนินการศึกษาแนวคิด ทฤษฎี และวรรณกรรมที่เกี่ยวข้องกับ ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ตั้งแต่ พ.ศ. 2559 – 2562

1.7 ประโยชน์ที่คาดว่าจะได้รับ

1. ประโยชน์ทางด้านวิชาการ

1. ทำให้ได้ข้อค้นพบในเชิงวิชาการเกี่ยวกับตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล
2. ทำให้ทราบถึงปัจจัยเหตุที่ส่งผลต่อความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล
3. ทำให้ทราบถึงผลของความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อผลการดำเนินงานของโซ่อุปทานดิจิทัล

2. ประโยชน์ต่อสังคม (การนำไปใช้)

1. การเปลี่ยนวิธีการปฏิบัติจากเดิมที่เป็นการป้องกันภัยคุกคามให้มาเป็นการเตรียมความพร้อมต่อภัยคุกคามจะส่งผลให้ธุรกิจสามารถที่จะดำเนินไปได้อย่างมีประสิทธิภาพและประสิทธิผล
2. องค์กรหรือบริษัทต่าง ๆ สามารถที่จะประเมินได้ถึงวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ว่าอยู่ในระดับใด เพื่อจะได้เตรียมความพร้อมต่อภัยคุกคามที่จะเข้ามาโจมตีองค์กรได้

1.8 นิยามศัพท์

ในการวิจัยในครั้งนี้ ผู้วิจัยได้ทำการนิยามศัพท์เฉพาะ ดังต่อไปนี้

1.8.1 ไซเบอร์ (Cyber) หมายถึง เป็นคำที่ใช้เติมหน้าคำอื่นเพื่อแสดงว่าเกี่ยวข้องกับระบบคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์ หรืออินเทอร์เน็ต หรือ ความเป็นจริงเสมือน (Virtual Reality) เช่น ไซเบอร์สเปซ (Cyberspace) หมายถึง สภาพแวดล้อมสมมติในเครือข่ายอินเทอร์เน็ต

1.8.2 ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) หมายถึง ภาวะพ้นจากภัยคุกคามที่มีต่อเครือข่ายระบบคอมพิวเตอร์ โปรแกรม และข้อมูล เพื่อรักษาไว้ซึ่งลักษณะสำคัญ 3 ประการ คือ ความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งาน ภาวะดังกล่าวจะเกิดขึ้นได้ต้องอาศัย บุคลากร กระบวนการทำงาน และเครื่องมือที่เหมาะสม

1.8.3 การคืนสภาพได้ (Resilience) หมายถึง เกี่ยวกับความสามารถที่จะกลับคืนสู่สภาพเดิมได้อย่างรวดเร็วและสามารถทำงานต่อไป

1.8.4 การคืนสภาพได้ทางไซเบอร์ (Cyber Resilience) หมายถึง สภาวะที่องค์กรมีความทนทาน คล่องตัว และมีความสามารถที่จะดำเนินงานต่อไปได้ แม้จะประสบปัญหาจากภัยคุกคามที่คาดไม่ถึงทางระบบอินเทอร์เน็ต เป็นแนวทางในการเตรียมความพร้อมขององค์กรให้สามารถป้องกัน ต่อต้าน ตรวจจับและตอบสนองต่อการบุกรุก การจารกรรม หรือการหลอกลวงที่จะทำให้หน่วยงานเสียหายได้

1.8.5 โซ่อุปทานดิจิทัล (Digital Supply Chain) หมายถึง กระบวนการการใช้เทคโนโลยีที่มีความชาญฉลาดและเหมาะสมในการสนับสนุนและประสานกระบวนการและกิจกรรมทั้งหมดของโซ่อุปทาน เป็นระบบที่มีความสามารถในการจัดการข้อมูลที่มีขนาดใหญ่ เป็นระบบที่ต้องอาศัยความร่วมมือกัน การติดต่อสื่อสาร เพื่อรองรับและประสานการทำงานร่วมกันระหว่างองค์กรที่มีข้อมูลที่เป็นดิจิทัลมากขึ้น

1.8.6 ตัวแบบวุฒิภาวะความสามารถ (Capability Maturity Model) หมายถึง เป็นต้นแบบของการวัดวุฒิภาวะความสามารถในการทำงาน ความสำเร็จในการทำงานใดๆ ในอนาคตของบริษัทหรือหน่วยงาน ขึ้นอยู่กับระดับวุฒิภาวะความสามารถ ในการทำงานของบริษัท หรือหน่วยงานนั้น ในทำนองเดียวกัน วุฒิภาวะความสามารถของบริษัทหรือหน่วยงานนั้น ก็ขึ้นอยู่กับผลการทำงานในอดีตของบริษัทหรือหน่วยงานนั้น

1.8.7 วิสาหกิจขนาดกลางและขนาดย่อม (SMEs) หมายถึง ธุรกิจที่จดทะเบียนตามรายชื่อสถานประกอบการที่ได้รับอนุญาตให้ประกอบกิจการ ในปี พ.ศ. 2561 ที่สำนักงานส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม (สสว.) ให้การสนับสนุนและส่งเสริมที่จะครอบคลุมเฉพาะวิสาหกิจขนาดกลางและขนาดย่อม ในกิจการผลิตสินค้า กิจการให้บริการ และกิจการค้าส่งและค้าปลีก

1.8.8 ธุรกิจดิจิทัล ธุรกิจดิจิทัล คือแนวทางในการดำเนินธุรกิจที่จะเข้ามาเสริมพลังให้รูปแบบการติดต่อธุรกิจดั้งเดิม มีประสิทธิภาพและประสิทธิผลมากขึ้น อำนวยความสะดวกให้สินค้าและบริการสามารถเข้าถึงลูกค้าได้อย่างตรงกลุ่ม ทำให้การโต้ตอบทางธุรกรรมเป็นไปอย่างรวดเร็ว ประหยัดทรัพยากรทั้งทางด้านต้นทุนและเวลา โดยธุรกิจดิจิทัลที่ก่อนหน้านี้ได้มีการ

ปรับตัวไปบ้างแล้วจากการเข้ามาของ e-Business ดังนั้น รูปแบบการดำเนินธุรกิจดิจิทัลจะต้องสามารถปรับเปลี่ยนได้ตามบริบทที่เปลี่ยนแปลงไปได้อย่างรวดเร็วและไม่ควรยึดติดกับความสำเร็จในอดีต สามารถเชื่อมต่อและสื่อสารอย่างเป็นระบบระหว่างข้อมูลและหลักฐานเพื่อแสดงข้อเท็จจริงว่าธุรกิจสร้างคุณค่าและส่งมอบคุณค่าให้กับลูกค้าได้อย่างไร ซึ่งสัมพันธ์กับการสร้างรายได้ การบริหารต้นทุนและกำไรของบริษัทเพื่อให้เกิดการตัดสินใจอย่างมีเหตุมีผล และเมื่อมีข้อมูลที่สามารถสร้างการเปลี่ยนแปลงใหม่ๆ พร้อมกับความก้าวหน้าทางเทคโนโลยีด้านการติดต่อสื่อสาร

1.9 สรุป

เนื้อหาในบทที่ 1 ผู้วิจัยได้สรุปถึงที่มาความสำคัญรวมถึงช่องว่างของประเด็นปัญหาในด้านการคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานที่ควรได้รับการพัฒนา ทั้งในมุมมองปัญหาในโลกปัจจุบันที่ต้องเผชิญต่อภัยคุกคามทางไซเบอร์ และมุมมองด้านวิชาการที่ยังคงต้องการการศึกษาเพิ่มเติม โดยสรุปประเด็นปัญหาที่ผู้วิจัยได้เล็งเห็นมีอยู่ 4 ประการหลัก ๆ นั่นคือ 1) การวิจัยทางด้านการคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานยังมีอยู่อย่างจำกัด 2) จากการศึกษาเบื้องต้นพบว่าการคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานยังไม่มีทิศทางที่ชัดเจนในการปฏิบัติและการพัฒนา 3) จากการศึกษามาตรฐานและกรอบแนวคิดด้านการคืนสภาพได้ของโซ่อุปทาน ยังไม่พบกรอบแนวคิดหรือมาตรฐานใดที่มีการบูรณาการภายใต้การดำเนินกิจกรรมทางด้านไซเบอร์ และ 4) จากนโยบายของรัฐบาลที่ต้องการผลักดันให้ประเทศไทยเข้าสู่ยุคประเทศไทย 4.0 ซึ่งเป็นยุคที่เศรษฐกิจจะถูกขับเคลื่อนด้วยนวัตกรรม การเตรียมความพร้อมต่อภัยคุกคามทางไซเบอร์หรือให้ โซ่อุปทานมีการคืนสภาพได้ทางไซเบอร์จึงมีความจำเป็นที่ต้องได้รับการศึกษาและพัฒนากรอบแนวคิดที่เหมาะสมต่อวิสาหกิจขนาดกลางและขนาดย่อม การศึกษาผู้วิจัยได้ทำการศึกษาปัจจัยที่มีผลต่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล โดยนำผลที่ได้จากการศึกษาบางส่วนมาร่วมกับการทบทวนวรรณกรรมเพิ่มเติมเพื่อหาองค์ประกอบในการพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล โดยได้พัฒนาตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ตัวชี้วัดการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล จากนั้นนำผลที่ได้จากการศึกษามาดำเนินการในการประเมินตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์โดยไปทำการสัมภาษณ์เชิงลึกจากผู้เชี่ยวชาญจำนวน 17 ท่าน เพื่อยืนยันถึงความเหมาะสมขององค์ประกอบของตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล โดยนำผลที่ได้

จากการสัมภาษณ์เชิงลึกมาทำการวิเคราะห์เชิงเนื้อหาเพื่อยืนยันถึงผลที่ได้จากการสัมภาษณ์เชิงลึก และผลจากการสัมภาษณ์เชิงลึกยังมีประเด็นในบางประเด็นสำหรับการศึกษาที่หาคำตอบได้ไม่ชัดเจนนัก จึงได้นำประเด็นเหล่านั้นมาทำการสนทนากลุ่มเพื่อโดยผู้ทรงคุณวุฒิจำนวน 7 ท่าน และนำผลที่ได้มาทำการพัฒนาเป็นตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลเพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล และพัฒนาเป็นระบบประเมินเพื่อให้วิสาหกิจขนาดกลางและขนาดย่อมนำไปใช้งานต่อไป