บทที่ 5
สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

การศึกษาและวิจัยในครั้งนี้เป็นการพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม โดยผู้วิจัยได้กำหนดให้มีวัตถุประสงค์ 6 ข้อ ดังต่อไปนี้ 1) เพื่อทำการศึกษาและวิเคราะห์ระดับการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล 2) เพื่อทำการวิเคราะห์ปัจจัยสำคัญที่มีผลต่อความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล 3) เพื่อพัฒนาตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล 4) เพื่อพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล 5) เพื่อทำการประเมินตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่มีผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล และ 6) เพื่อพัฒนาระบบการประเมินระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่มีผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม การวิจัยได้ใช้ระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative Research) โดยวิธีวิเคราะห์เนื้อหาการสัมภาษณ์เชิงลึกและการสนทนากลุ่ม และเชิงปริมาณ (Quantitative Research) โดยการสำรวจความคิดเห็นของกลุ่มตัวอย่าง ผู้วิจัยจะขอสรุปผลการวิจัยโดยแบ่งตามวัตถุประสงค์ของการศึกษาตามลำดับดังต่อไปนี้

5.1 สรุปผลการวิจัย

5.1.1 ผลการศึกษาตามวัตถุประสงค์ข้อที่ 1 เพื่อทำการวิเคราะห์ปัจจัยสำคัญที่มีผลต่อความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ในการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

ผู้วิจัยได้ทำการศึกษาปัจจัยที่สำคัญที่มีผลต่อความสามารถในการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทาน เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล โดยกลุ่มประชาการที่ใช้ใน

การศึกษา ได้แก่วิสาหกิจขนาดกลางและขนาดย่อม (SME) ในประเทศไทย 3,077,822 ราย โดยแบ่งเป็น 4 กลุ่มธุรกิจได้แก่ ภาคการค้า ภาคการบริการ ภาคการผลิต และภาคธุรกิจการเกษตร กลุ่มตัวอย่างผู้วิจัยได้ส่งแบบสอบถามไปยังวิสาหกิจขนาดกลางและขนาดย่อม 400 บริษัท และได้ส่งจำนวนแบบสอบถามบริษัทละ 5 ฉบับ รวมทั้งสิ้น 2,000 ฉบับ ผลการตอบแบบสอบถามกลับได้จำนวนแบบสอบถามที่ตอบกลับมา 1,864 ฉบับ คิดเป็นร้อยละ 93.2 ผู้วิจัยได้ออกแบบสอบถามซึ่งเป็น 8 ส่วน ได้แก่ ส่วนที่ 1 คือข้อมูลทั่วไปขององค์กรของผู้ตอบแบบสอบถาม ส่วนที่ 2 คือ ข้อมูลเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริษัทของผู้ตอบแบบสอบถาม ส่วนที่ 3 คือ ความคิดเห็นเกี่ยวกับความสามารถการคืนสภาพได้ทางด้านไซเบอร์ของโซ่อุปทานดิจิทัล ส่วนที่ 4 คือ ความคิดเห็นเกี่ยวกับความร่วมมือกันของโซ่อุปทาน ส่วนที่ 5 คือ ความคิดเห็นเกี่ยวกับการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล ส่วนที่ 6 คือความคิดเห็นเกี่ยวกับการจัดการเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล ส่วนที่ 7 คือ ข้อมูลสภาพการดำเนินงานที่เกี่ยวข้องกับการจัดการความต่อเนื่องทางธุรกิจดิจิทัล และส่วนที่ 8 คือ ข้อเสนอแนะอื่น ๆ

ผลการศึกษาสำหรับข้อมูลทั่วไปขององค์กรของผู้ตอบแบบสอบถามพบว่า วิสาหกิจขนาดกลางและขนาดย่อม ในประเทศไทยส่วนใหญ่เป็นองค์กรธุรกิจในภาคการค้า มีระยะเวลาในการดำเนินการ 10 ปีขึ้นไป จำนวนพนักงาน 200 คนขึ้นไป ธุรกิจส่วนใหญ่จะมีตลาดอยู่ในระดับประเทศ มีพนักงานตำแหน่งพนักงานปฏิบัติการ โดยพนักงานที่รู้ IT ที่ประมาณ 61-70% ตามลำดับ ด้านผลการสอบถามในส่วนของการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร พบว่าบริษัทส่วนใหญ่ได้รับรายงานจากพนักงานน้อยครั้งมากเมื่อพนักงานตกเป็นเหยื่อจากการโจมตีทางไซเบอร์ บริษัทส่วนใหญ่มีแผนฉุกเฉินในการรับมือต่อเหตุการณ์การโจมตีทางไซเบอร์ มีความเข้มงวดเกี่ยวกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นบ้างครั้ง และมีการทบทวนเกี่ยวกับนโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศเป็นบางครั้ง

ผลจากการสอบถามในเรื่องระบบการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่องค์กรใช้อยู่ในปัจจุบัน พบว่าบริษัทส่วนใหญ่โปรแกรมป้องกันไวรัส (Anti-virus Software) ใช้ในการรักษาความมั่นคงปลอดภัยไซเบอร์ มากที่สุด รองลงมาจะใช้ไฟร์วอลล์ (Firewall) โปรแกรมการจัดการลงบันทึกเข้าออก (Log Management Software) ผลการสอบถามในเรื่องรูปแบบการติดตามผลการปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ พบว่า การตรวจสอบความมั่นคงปลอดภัยโดยบุคลากรภายในองค์กร (Security Audits by Internal Staff) เป็นรูปแบบการติดตามผลการปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์มากที่สุด รองลงมา คือ การทดสอบหาความบกพร่องด้านความมั่นคงปลอดภัย ไซเบอร์ขององค์กรโดยบุคลากรภายในองค์กร (Penetration Testing by Internal Staff) ตรวจสอบความมั่นคงปลอดภัยไซเบอร์โดยองค์กรภายนอก (Security Audits by

External Organization) และผลการสอบถามในเรื่องนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ที่ SMEs ได้ดำเนินการอยู่ในปัจจุบัน พบว่า มีแผนพัฒนาความต่อเนื่องทางด้านเทคโนโลยีสารสนเทศเป็นรูปแบบการติดตามผลการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ มากที่สุด รองลงมาคือ มีการควบคุมเกี่ยวกับซอฟต์แวร์ที่มีการละเมิดลิขสิทธิ์ มีการเก็บรักษาสื่อ อุปกรณ์ในการสำรองข้อมูล มีการจัดการสื่อทางคอมพิวเตอร์ที่สามารถถอดได้ (ตัวอย่างเช่น USB) มีมาตรการในการรักษาความมั่นคงปลอดภัยสำหรับการนำเอาอุปกรณ์ส่วนตัวมาใช้

สำหรับผลการวิจัยเพื่อทำการวิเคราะห์ปัจจัยสำคัญที่มีผลต่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล พบว่า การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล ความร่วมมือกันของโซ่อุปทานดิจิทัล และการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล เป็นปัจจัยที่มีผลต่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลในระดับมาก ส่วนการวิเคราะห์ข้อมูลของวิสาหกิจขนาดกลางและขนาดย่อมเกี่ยวกับการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความต่อเนื่องทางธุรกิจดิจิทัล พบว่า วิสาหกิจขนาดกลางและขนาดย่อม มีการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความต่อเนื่องทางธุรกิจดิจิทัลอยู่ในระดับมาก

ผลการวิจัยเพื่อศึกษาความสัมพันธ์โครงสร้างเชิงสาเหตุของปัจจัยที่ส่งผลต่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล สำหรับวิสาหกิจขนาดกลางและขนาดย่อม พบว่า ความร่วมมือกันของโซ่อุปทานดิจิทัล มีอิทธิพลทางตรงเชิงบวกต่อการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล และมีอิทธิพลทางอ้อมเชิงบวกต่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และมีอิทธิพลทางอ้อมเชิงบวกต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล การจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล มีอิทธิพลทางตรงเชิงบวกต่อการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล และมีอิทธิพลทางอ้อมเชิงบวกต่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และมีอิทธิพลทางอ้อมเชิงบวกต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล มีอิทธิพลทางตรงเชิงบวกต่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล และมีอิทธิพลทางอ้อมเชิงบวกต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล และการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล มีอิทธิพลทางตรงเชิงบวกต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

ผลการศึกษาโมเดลปัจจัยเชิงโครงสร้างที่มีผลต่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล สำหรับวิสาหกิจขนาดกลางและขนาดย่อม พบว่า ปัจจัยความร่วมมือกันของโซ่อุปทานดิจิทัล ปัจจัยการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล และปัจจัยการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล เป็นปัจจัยที่มีอิทธิพลโดยตรงต่อการคืนสภาพได้ทาง

ไซเบอร์ของโซ่อุปทานดิจิทัล ปัจจัยความร่วมมือกันของโซ่อุปทานดิจิทัล และปัจจัยการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล เป็นปัจจัยที่มีอิทธิพลโดยตรงต่อการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล และปัจจัยการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เป็นปัจจัยที่มีอิทธิพลโดยตรงต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

5.1.2 ผลการศึกษาตามวัตถุประสงค์ข้อที่ 2&3 เพื่อพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในขั้นตอนนี้ผู้วิจัยได้ทำการศึกษาถึงเอกสารและงานวิจัยที่เกี่ยวข้องกับงานวิจัยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ การคืนสภาพได้ทางไซเบอร์ ความมั่นคงปลอดภัยของโซ่อุปทาน การจัดการความต่อเนื่องทางธุรกิจ และตัวแบบวุฒิภาวะความสามารถ โดยได้ศึกษาถึง มาตรฐาน (Standard) กรอบแนวคิด (Framework) แบบการปฏิบัติที่ดีที่สุด (Best Practice) ที่เกี่ยวข้องกับการคืนสภาพได้ทางไซเบอร์ที่มีอยู่ในปัจจุบัน เพื่อพัฒนาตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล โดยผู้วิจัยแบ่งขั้นตอนในการศึกษา 3 ขั้นตอนดังต่อไปนี้

ขั้นที่ 1 การศึกษาแนวทางในการกำหนดตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Model)

โดยการศึกษาผู้วิจัยได้อิงกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐอเมริกา (NIST) ที่พัฒนาโดยยึดหลักตามมาตรฐาน CIS CSC (Council on Cybersecurity: 20 Critical Security Controls), COBIT 5, ISA 62443-2-1: 2009, ISA 62443-3-3: 2013, ISO/IEC 27001:2013 และ NIST SP 800-53 Rev. 4 จากนั้นผู้วิจัยได้ทำการศึกษาเพิ่มเติมเกี่ยวกับวุฒิภาวะความสามารถบูรณาการ (Capability Maturity Model Integration: CMMI) มาตรฐาน ISO/IEC 27002:2013 ข้อปฏิบัติสำหรับสนับสนุน ISO 27001 ซึ่งระบุแนวทางปฏิบัติที่ดีที่สุด (Best Practice) สำหรับการเริ่มต้น การพัฒนา และการบำรุงรักษา ISMS มาตรฐาน ISO/IEC 27005:2018 มาตรฐานด้านการบริหารจัดการความเสี่ยงด้านไซเบอร์ ที่ประกอบด้วย Information technology, Security techniques, Information security management systems มาตรฐาน ISO 22301:2012 มาตรฐานด้านการบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management Systems) เป็นมาตรฐานที่ช่วยให้แต่ละองค์กรสามารถวางแผนรับมือกับภัยพิบัติรูปแบบต่าง ๆ ได้อย่างเป็นระบบ มาตรฐาน ISO/IEC 27032:2012 ส่วนขยายของ ISO 27001 ซึ่งเกี่ยวข้องในเรื่อง Confidentiality, Integrity และ Availability กับความมั่นคงปลอดภัยของทรัพย์สินในโลกไซเบอร์ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล บริการ รวมไปถึงสิ่งที่จับต้องไม่ได้ (Virtual Assets) เช่น ชื่อเสียง เป็นต้น มาตรฐาน IS/IEC 28000 เป็นมาตรฐานที่กำหนด

ข้อกำหนดของระบบการจัดการความมั่นคงปลอดภัยของโซ่อุปทาน และจัดเตรียมรูปแบบการจัดการให้กับองค์กรที่ต้องการนำระบบนี้ไปใช้ มีจุดมุ่งหมายในการจัดการความเสี่ยงอย่างมีประสิทธิภาพ โดยจัดกิจกรรมขององค์กรด้านความมั่นคงปลอดภัยของโซ่อุปทานภายใต้ระบบเดียวกับระบบการจัดการอื่น ๆ และมาตรฐาน ISO 31000:2009 มาตรฐานด้านการบริหารจัดการความเสี่ยงระดับองค์กร มาร่วมใช้สำหรับการพัฒนากรอบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

มาตรฐานต่าง ๆ ที่ใช้ ในการศึกษานี้ คือ เป็นมาตรฐานสากลที่ใช้สำหรับระบบการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่มีผลทำให้กระบวนการทำงานขององค์กรภายใต้โซ่อุปทานดิจิทัล สามารถที่จะทำงานได้อย่างมีความปลอดภัยจากสภาพแวดล้อมทางดิจิทัลที่เป็นอยู่ในปัจจุบัน ด้วยการทำงานที่มีขั้นตอนชัดเจน และมีความพร้อมในเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ในโซ่อุปทานดิจิทัลได้อย่างมีประสิทธิภาพ สร้างความเชื่อถือคู่ค้าที่อยู่ภายใต้โซ่อุปทานดิจิทัล จากการศึกษาข้อมูลดังกล่าวข้างต้นทำให้ผู้วิจัยสามารถนำเสนอตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Model) ที่ได้พัฒนาขึ้น ซึ่งประกอบด้วย 6 หมวด 32 มิติ

ขั้นที่ 2 การศึกษาแนวทางในการกำหนดตัวชี้วัดการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Indicator)

การศึกษาในขั้นนี้ผู้วิจัยได้ทำการพัฒนาตัวชี้วัดการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล โดยพิจารณาจากการนำเอามิติของแต่ละหมวด ไปทำการทบทวนวรรณกรรมเพื่อดำเนินการในการจัดทำตัวชี้วัดของแต่ละมิติ จากผลของการดำเนินการดังกล่าวทำให้ผู้วิจัยสามารถกำหนดตัวชี้วัดจากบทความจำนวนรวมทั้งสิ้น 135 บทความ โดยบทความจะเป็นบทความที่เกี่ยวข้องคำมิติในแต่หัวข้อ จากผลการทบทวนวรรณกรรม ทำให้ได้ตัวชี้วัดทั้งหมดเป็นจำนวน 142 ตัวชี้วัด แบ่งเป็น การจัดการสินทรัพย์ (Asset Management) 5 ตัวชี้วัด สภาพแวดล้อมทางธุรกิจ (Business Environment) 3 ตัวชี้วัด การกำกับดูแล (Governance) 5 ตัวชี้วัด การประเมินความเสี่ยง (Risk Assessment) 7 ตัวชี้วัด กลยุทธ์การจัดการความเสี่ยง (Risk Management Strategy) 3 ตัวชี้วัด การจัดการความเสี่ยงของโซ่อุปทาน (Supply Chain Risk Management) 6 ตัวชี้วัด กลยุทธ์ความมั่นคงปลอดภัยของโซ่อุปทาน (Supply Chain Security Strategy) 4 ตัวชี้วัด การจัดการการระบุตัวตน การยืนยันตัวตน และการควบคุมการเข้าถึง (Identity Management, Authentication and Access Control) 10 ตัวชี้วัด การตระหนักและการฝึกอบรม (Awareness and Training) 4 ตัวชี้วัด ความมั่นคงปลอดภัยของข้อมูล (Data Security) 3 ตัวชี้วัด ขั้นตอนและกระบวนการการป้องกันข้อมูล (Information Protection Processes and Procedures) 11 ตัวชี้วัด การดูแลบำรุงรักษา

(Maintenance) 3 ตัวชี้วัด เทคโนโลยีการป้องกัน (Protective Technology) 8 ตัวชี้วัด ความเป็นส่วนบุคคล (Privacy) 6 ตัวชี้วัด เหตุการณ์ความผิดปกติ (Anomalies and Events) 5 ตัวชี้วัด การเฝ้าระวังความมั่นคงปลอดภัยอย่างต่อเนื่อง (Security Continuous Monitoring) 4 ตัวชี้วัด กระบวนการการตรวจจับ (Detection Processes) 5 ตัวชี้วัด ข่าวกรองทางไซเบอร์ (Cyber Intelligence) 2 ตัวชี้วัด การวางแผนการรับมือ (Response Planning) 2 ตัวชี้วัด การสื่อสาร (Communications) 4 ตัวชี้วัด การวิเคราะห์ (Analysis) 5 ตัวชี้วัด การบรรเทา (Mitigation) 4 ตัวชี้วัด การพัฒนา (Improvements) 1 ตัวชี้วัด ความคล่องตัวของโซ่อุปทาน (Supply Chain Agility) 4 ตัวชี้วัด การวางแผนการฟื้นฟู (Recovery Planning) 2 ตัวชี้วัด การพัฒนา (Improvements) 1 ตัวชี้วัด การสื่อสาร (Communications) 3 ตัวชี้วัด กลยุทธ์ความคงทน (Robust Strategy) 5 ตัวชี้วัด ความยั่งยืนของโซ่อุปทาน (Supply Chain Sustainability) 3 ตัวชี้วัด ความเชื่อถือได้ของโซ่อุปทาน (Dependability of Supply Chain) 6 ตัวชี้วัด แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan) 5 ตัวชี้วัด และการประเมินความต่อเนื่องทางธุรกิจ (Business Continuity Assessment) 3 ตัวชี้วัด

ขั้นที่ 3 การศึกษาแนวทางในการกำหนดระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Maturity Level for Cyber Resilience Supply Chains)

เป็นการศึกษาเพื่อการกำหนดระดับวุฒิภาวะความสามารถสำหรับการสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทาน ผู้วิจัยได้ทำการนิยามระดับของวุฒิภาวะความสามารถสำหรับการสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทาน โดยยึดหลักจากมาตรฐานตัวแบบ Capability Maturity Model Integration (CMMI) และมาตรฐาน ISO/IEC 15504 โดยได้กำหนดให้มีระดับวุฒิภาวะความสามารถ 5 ระดับได้แก่ ระดับที่ 1 (Level 1) ระดับเริ่มต้น (Initial Level) เป็นระดับที่บริษัทต่างๆ ต้องจัดการต่อภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล โดยอาศัยความสามารถของบุคลากรเพียงอย่างเดียว ซึ่งมีลักษณะของการทำงานที่ยังไม่เป็นทางการมากนัก ยังไม่มีการควบคุมที่ดี ไม่มีการวางแผนงานที่เป็นระบบ จึงทำให้ไม่สามารถประเมินคุณภาพในการรักษาความปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่เกิดขึ้นว่าจะมีคุณภาพดีหรือไม่ ระดับที่ 2 (Level 2) ระดับจัดการเบื้องต้น (Repeatable Level) ในระดับนี้มีแนวทางในการจัดการต่อภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัลเบื้องต้น มีการวางแผนการทำงานอย่างเป็นระบบ มีการจัดทำเอกสาร สามารถตรวจสอบ และนำไปปฏิบัติได้ บริษัทต่าง ๆ สามารถเข้าสู่ระดับนี้ได้ จะสามารถจัดการต่อปัญหาภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่มีลักษณะแบบเดียวกันให้ประสบผลสำเร็จได้เช่นเดียวกับภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่สามารถจัดการได้สำเร็จไปแล้ว ระดับที่ 3 (Level 3) ระดับที่มีการกำหนดกระบวนการขึ้นอย่างชัดเจน (Defined Level) ในระดับนี้เป็นการพัฒนาเพิ่มขึ้นจาก Repeatable Level การเข้าสู่ระดับบริษัทต่าง ๆ จะต้องมีการกำหนดแนวทางใน

การปฏิบัติงานด้านการจัดทำเอกสารและกำหนดมาตรฐานในการปฏิบัติงาน ในด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัลได้อย่างเหมาะสม โดยมาตรฐานดังกล่าวต้องมีแนวปฏิบัติแบบเดียวกันทั้งองค์กร นั้นคือ องค์กรเริ่มมีระเบียบวิธีการปฏิบัติงานเป็นมาตรฐานของตนเอง ระดับที่ 4 (Level 4) ระดับมีการจัดการ (Managed Level) เป็นการพัฒนาเพิ่มขึ้นจาก Defined Level ลักษณะการปฏิบัติในระดับนี้ผู้จัดทำต้องมีการรวบรวมข้อมูล รายละเอียดการปฏิบัติงานต่าง ๆ ที่เกิดขึ้นไว้ในรูปของสถิติ (Statistical Process Control) เพื่อนำข้อมูลนั้นมาใช้ในการศึกษาวิเคราะห์ผลการทำงาน สามารถวัดผล และควบคุมกระบวนการในการจัดการความมั่นคงปลอดภัยทางไซเบอร์ของโซ่อุปทานดิจิทัล และระดับที่ 5 (Level) ระดับปรับปรุงให้เหมาะสมที่สุด (Optimizing Level) เป็นระดับที่ได้นำเอาหลักการจัดการคุณภาพ (Continuous Process Improvement) มาใช้ เพื่อป้องกันไม่ให้เกิดข้อบกพร่องในการปฏิบัติงาน และนำไปสู่การพัฒนาอย่างต่อเนื่อง รวมถึงเพื่อให้บริษัทต่าง ๆ สามารถปรับเปลี่ยนตัวเองให้สอดคล้องกับการเปลี่ยนแปลงทางด้านเทคโนโลยีได้

จากการวิเคราะห์และสังเคราะห์ ตัวแบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล (Cyber-Resilient Supply Chain Model) ตัวชี้วัดการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล (Cyber Resilience Supply Chain Indicator) เพื่อมาพัฒนาให้เป็น ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล (Capability Maturity Model for Cyber-Resilient Supply Chain) สำหรับการจัดการความต่อเนื่องทางธุรกิจดิจิทัลของโซ่อุปทานดิจิทัลนั้น ทำให้ผู้วิจัยได้กำหนดถึงองค์ประกอบและตัวชี้วัดภายในที่แสดงถึงระดับความสามารถของวิสาหกิจขนาดกลางและขนาดย่อม ในการตอบสนองต่อภัยคุกคามที่เข้ามาโจมตีและความสามารถในการคืนสภาพได้ทางไซเบอร์ ซึ่งคะแนนที่ได้รับจากการประเมินผลของบุคลากรของวิสาหกิจขนาดกลางและขนาดย่อมในฐานะตัวแทนองค์กร ที่ผ่านทั้ง 32 มิติการดำเนินงาน ทำให้สามารถแสดงถึงระดับวุฒิภาวะความสามารถสำหรับการคืนสภาพได้ด้านไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัลต่อไป

5.1.3 ผลการศึกษาตามวัตถุประสงค์ข้อที่ 4 เพื่อทำการประเมินตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่มีผลต่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล ประกอบไปด้วย 3 ขั้นตอนหลัก ได้แก่

5.1.3.1 การสัมภาษณ์เชิงลึกผู้เชี่ยวชาญเพื่อการประเมินผลเกี่ยวกับแนวทางในการกำหนดตัวแบบ ตัวชี้วัด และเกณฑ์การประเมินระดับวุฒิภาวะความสามารถในการสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการจัดการความต่อเนื่องทางธุรกิจดิจิทัล

ผู้วิจัยใช้ระเบียบวิธีดำ เนินงานวิจัยเชิงคุณภาพ (Qualitative Research) ด้วยวิธีการสัมภาษณ์เชิงลึก (In-depth Interview) โดยพัฒนาแบบสัมภาษณ์แบบกึ่งโครงสร้าง (Semi-Structure Interview) ซึ่งมีการกำหนดประเด็นคำถามส่วนหนึ่งตามกรอบแนวคิดและมีคำถามเกิดขึ้นใหม่ระหว่างการสัมภาษณ์เป็นลักษณะซักไซ้ไล่เลียงเพื่อให้ทราบข้อมูลในเรื่องนั้นให้มากที่สุด โดยข้อมูลที่ได้รับการจากการสัมภาษณ์ ผู้วิจัยได้รับความอนุเคราะห์ข้อมูลจากผู้เชี่ยวชาญ 17 ท่าน จากกลุ่มสาขา 4 กลุ่มสาขา ได้แก่ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) จำนวน 4 ท่าน ด้านตัวแบบวุฒิภาวะความสามารถ (Capability Maturity Model: CMM) จำนวน 4 ท่าน ด้านเทคโนโลยีดิจิทัล (Digital Technology) จำนวน 5 ท่าน และด้านโลจิสติกส์และโซ่อุปทาน จำนวน 4 ท่าน โดยมีวัตถุประสงค์เพื่อตรวจสอบกรอบแนวคิด ตัวชี้วัด รวมไปถึงเกณฑ์ที่จะนำมาใช้ในการประเมินระบบระดับวุฒิภาวะความสามารถในการสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทาน เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจทัล ในวิสาหกิจขนาดกลางและขนาดย่อมว่าเป็นไปตามที่ได้ศึกษาหรือไม่ และเพื่อรับทราบถึงประสบการณ์ ตลอดจนแนวปฏิบัติในการกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์ บนพื้นฐานของการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อมต่อไป

5.1.3.2 การทดสอบความเหมาะสมและความสอดคล้องของตัวแบบ ตัวชี้วัด และเกณฑ์การประเมินระดับวุฒิภาวะความสามารถในการสร้างการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล ผู้วิจัยใช้การวิเคราะห์เนื้อหา (Content Analysis) มาตรวจสอบและผลการสัมภาษณ์ของผู้เชี่ยวชาญที่ได้ไปดำเนินการสัมภาษณ์เชิงลึกมาตามข้อที่ 5.1.3.1 เพื่อวินิจฉัยถึงความเหมาะสมและความสอดคล้องของตัวแบบ ตัวชี้วัดระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล และเกณฑ์ในการประเมินระดับวุฒิภาวะที่ได้พัฒนาขึ้น

5.1.3.3 การยืนยันตัวแบบ ตัวชี้วัด และเกณฑ์การประเมินระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล ผู้วิจัยใช้การสนทนากลุ่ม (Focus Group) โดยดำเนินการโดยได้รับความอนุเคราะห์จากผู้ทรงคุณวุฒิจำนวน 7 ท่าน เพื่อตอบประเด็นข้อคำถามที่เกิดขึ้นเพิ่มเติมมาจากการสัมภาษณ์เชิงลึก (In-depth interview) ที่ผู้วิจัยได้ไปสัมภาษณ์ผู้เชี่ยวชาญมาแล้วจากข้อที่ 5.1.3.1 โดยประเด็นข้อคำถามเพิ่มเติมนั้นมีอยู่ด้วย 7 ประเด็นข้อคำถาม และผลจากการสนทนากลุ่มปรากฏว่าผู้ทรงคุณวุฒิทุกท่าน ได้ให้ความเห็นชอบในประเด็นข้อคำถามดังกล่าว ถึงความเหมาะสมของงานวิจัยที่ผู้วิจัยได้นำเสนอในครั้งนี้ ดังนั้นจากผลการวิจัยทั้งหมดจึงยืนยันได้ว่า งานวิจัยที่ผู้วิจัยนำเสนอในครั้งนี้สามารถดำเนินการให้เป็นรูปธรรมได้ และสามารถทำให้เกิดประโยชน์ต่อผู้ประกอบการต่อไป

5.1.4 ผลการศึกษาตามวัตถุประสงค์ข้อที่ 5 เพื่อพัฒนาระบบการประเมินระดับวุฒิภาวะความสามารถการคืนสภาพได้ทางด้านไซเบอร์ของห่วงโซ่อุปทานดิจิทัล ที่มีผลต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม

จากผลการศึกษาที่ได้ตามวัตถุประสงค์ในข้อที่ 3-5 นั้น ผู้วิจัยได้นำความรู้ที่ได้ค้นพบมาทำการต่อยอดเพื่อให้สามารถประยุกต์ใช้ความรู้จากงานวิจัยฉบับนี้ได้อย่างเป็นรูปธรรม โดยการพัฒนาระบบประเมินในรูปแบบมาโคร (Macro) บนโปรแกรมไมโครซอฟท์ เอ็กซ์เซล (Microsoft Excel) เพื่อให้เกิดความสะดวกในการประเมิน และยังจะสามารถวิเคราะห์ช่องว่าง (Gap Analysis) ในแต่ละมิติ รวมไปถึงภาพรวมของแต่ละหมวด เพื่อให้ผู้บริหารได้เห็นถึงช่องว่างของจุดแข็งและจุดที่ควรพัฒนาของการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ที่มีผลต่อการจัดการความต่อเนื่องของธุรกิจดิจิทัล เพื่อเป็นส่วนสนับสนุนในการตัดสินใจในการลงทุนด้านไอทีขององค์กร/หน่วยงาน เพื่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลต่อไป นอกจากนี้ระบบยังจะสามารถให้คำแนะนำสำหรับมิติที่เป็นจุดที่ควรพัฒนาแก่ผู้บริหาร เพื่อเป็นแนวทางในการปรับปรุงระบบการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานขององค์กร/หน่วยงานได้อย่างมีทิศทาง มีเป้าหมาย และมีประสิทธิภาพ

5.2 อภิปรายผลการวิจัย

ผลการวิจัยที่ได้ ผู้วิจัยสามารถนำประเด็นที่น่าสนใจมาอภิปรายผลดังต่อไปนี้

1) ความร่วมมือกันของโซ่อุปทานดิจิทัล มีอิทธิพลโดยตรงต่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ซึ่งสอดคล้องกับผลการศึกษาของ Banomyong R. (2018) ที่พบว่า ความร่วมมือทางด้านเทคโนโลยีไม่ได้มองแต่ในเรื่องของการเปลี่ยนแปลงทางด้านวัฒนธรรมเท่านั้น จำเป็นต้องตระหนักถึง การไว้วางใจซึ่งกันและตลอดจนการแบ่งปันข้อมูลร่วมกันด้วยรวมไปถึงต้องหันมาสนใจต่อการดำเนินงานภายใน เพื่อที่จะได้รับมือกับการทำงานที่จะต้องติดต่อกับองค์กรที่อยู่ภายนอก เพราะข้อมูลที่เป็นความลับของบริษัทที่เพิ่มขึ้นจะทำให้เกิดการรั่วไหลของความรู้และการรั่วไหลของข้อมูลมากขึ้น เช่นเดียวกับงานวิจัยของสุธาทิพย์ เลิศวิวัฒน์ชัยพร และคณะ (2561) ที่พบว่า การปรับเปลี่ยนจากห่วงโซ่อุปทานแบบดั่งเดิมไปสู่รูปแบบใหม่ การแลกเปลี่ยนข้อมูลกับผู้มีส่วนได้ส่วนเสียจนรู้ถึงความต้องการของตลาด ทำให้เกิดการวางแผนงานไว้อย่างมีประสิทธิภาพ ทำให้เกิดความสัมพันธ์ภายในโซ่อุปทาน ระหว่างผู้จัดหาวัตถุดิบ พ่อค้า/ผู้รับซื้อ ผู้คัดเลือกวัตถุดิบให้กับโรงงานซึ่งตรงตามความต้องการของลูกค้า มีการจัดส่งวัตถุดิบที่ดีมีคุณภาพการส่งสินค้าให้ตรงต่อเวลาและปลอดภัย รวมไปถึงรูปแบบการสื่อสารเพื่อสร้างการรับรู้เกี่ยวกับอัตลักษณ์ของ

สินค้า ที่ต้องมีการสื่อสารให้ผู้บริโภครับทราบ โดยช่องทางของการสื่อสารผู้บริโภคต้องการที่จะรับรู้มากที่สุดคือการสื่อสารผ่าน ทางอินเตอร์เน็ตหรือออนไลน์ (Online)

2) การจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล มีอิทธิพลโดยตรงต่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ซึ่งสอดคล้องกับงานวิจัยของ Hassell et al. (2012) ที่พัฒนาชุดเครื่องมือในการสร้างแบบจำลองการป้องกันภัยคุกคามและช่องโหว่ทางไซเบอร์ เพื่อใช้ในการประเมินระบบและเครือข่ายเพื่อการพัฒนาให้เกิดการคืนสภาพได้ทางไซเบอร์ โดยในงานวิจัยได้มุ่งเน้นศึกษาถึงการนำเอาผลที่เกิดรับมือ โดยการสร้างตัวชี้วัดที่จะนำมาใช้ในการประเมินผลที่จะเกิดขึ้นต่อการคืนสภาพได้ของระบบเพื่อให้การออกแบบและการกำหนดค่าของขีดความสามารถของระบบในการรองรับการทำงานในสภาพไซเบอร์อย่างเหมาะสมสำหรับระบบและเครือข่ายต่อไปได้ เช่นเดียวกับงานวิจัยของ สุธาเทพ รุณเรศ (2561) ที่ศึกษาถึงปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต พบว่าลักษณะทางประชากรจะส่งผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ ซึ่งสามารถนำไปสร้างเป็นแนวทางในการกำหนดกลุ่มเป้าหมายถึงวิธีการในการป้องกันและลดความเสี่ยงจากภัยคุกคามของการโจมตีทางไซเบอร์ สามารถสร้างความตระหนักและความเข้าใจ ที่จะเกิดผลกระทบต่อตนเองจากอุปกรณ์ต่าง ๆ ในการเข้าถึงอินเทอร์เน็ตได้ อีกทั้งยังพบว่าปัจจัยด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต ถึงแม้ว่าการโจมตีทางไซเบอร์จะมีการพัฒนารูปแบบใหม่ ๆ เข้ามา และพยายามจะช่องโหว่เข้ามาโจมตีมากมายเพียงใด ผู้ใช้อินเทอร์เน็ตก็ไม่สามารถที่จะระวังได้ถึงภัยคุกคามทางไซเบอร์และไม่สามารถที่จะทางป้องกันจากการโจมตีที่เกิดขึ้นทั้งการโจมตีแบบเดิม ๆ หรือพัฒนาการโจมตีขึ้นมาแบบใหม่อันก่อให้เกิดความเสียหายที่ไม่สามารถคาดคิดได้ ซึ่งมีผลทำให้ไม่สามารถที่จะประเมินสถานการณ์ที่เกิดความเสียหายได้เช่นเดียวกัน รวมไปถึงประเด็นปัจจัยด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต หมายความว่า ผู้ที่มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์จะสามารถเข้าใจถึงปัญหาที่จะเกิดขึ้น รับรู้ได้ถึงความเสียหายที่เกิดขึ้นเมื่อถูกโจมตีทางเบอร์ โดยสามารถป้องกันเกี่ยวกับข้อมูลส่วนตัวที่ต้องเปิดเผยบนสาธารณะ เมื่อต้องมีการทำธุรกรรมออนไลน์ การติดตามข้อมูลข่าวสารการโจมตีรูปแบบใหม่ ๆ การดาวน์โหลดโปรแกรมที่ถูกต้องมาจากผู้ผลิตโดยตรงจะเป็นการช่วยป้องกันความเสี่ยงจากการแฝงตัวของไวรัสที่ไม่คาดคิดที่อาจติดมากับโปรแกรมได้ รวมถึงสามารถที่จะป้องกันภัยคุกคามจากผู้ไม่หวังดีที่จะเกิดผลกระทบต่อความเสียหายที่ไม่คาดคิดที่อาจเกิดขึ้นได้

3) การจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล มีอิทธิพลโดยตรงต่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล ซึ่งสอดคล้องกับงานวิจัยของ Tupaetal. (2017) การทำงานภายใต้โครงสร้างพื้นฐานด้านไอทีที่ซับซ้อน ความเสี่ยงอาจเกิดขึ้นได้ซึ่งเป็นผลมาจากว่าการทำงานร่วมกันระหว่างคน กระบวนการ และเทคโนโลยี ที่ได้กลายเป็นเครือข่ายที่มีความซับซ้อนมากขึ้น เช่นเดียวกับการศึกษาของ ปรัชญา เฉลิมวัฒน์ (2561) ได้ศึกษาเรื่อง แนวทางการพัฒนากาลังพลด้านไซเบอร์ เพื่อพร้อมรับภัยคุกคามระดับชาติ จากการศึกษาพบว่า ประเด็นเรื่องการขาดแคลนกำลังพลด้านไซเบอร์จะมาจากสาเหตุในเรื่องของประสบการณ์และความทุ่มเท ความยาก/สลับซับซ้อน/ปริมาณของเนื้อหาในการพัฒนา อบรมฝึกซ้อม ระยะเวลาที่ต้องใช้ในการพัฒนาบุคลากรไซเบอร์ ผู้บริหารไม่ให้ความสนใจอย่างจริงจัง เช่น บรรจุบุคคลที่ไม่มีความสามารถด้านไซเบอร์เข้ามาในตำแหน่ง ผู้บริหารหลงประเด็นไม่ได้คำนึงถึงเนื้องานที่หน่วยไซเบอร์ต้องปฏิบัติและแผนพัฒนากำลังพลด้านไซเบอร์ และปัญหาสมองไหลหรือการให้ค่าตอบแทนไม่คุ้มกับค่าขีดความสามารถ อีกทั้งยังได้มีนำเสนอแนวทางในการพัฒนากำลังพลด้านไซเบอร์เพื่อพร้อมรับภัยคุกคามไซเบอร์ในระดับชาติ โดยแนวทางดังกล่าวต้องมีความสอดคล้องกับยุทธศาสตร์ชาติในภาพรวม ยุทธศาสตร์ไซเบอร์ของชาติ เพื่อการพัฒนาบุคลากรด้านไซเบอร์ของประเทศให้มีความยั่งยืนและมีความเชื่อมั่นในการนำไปปฏิบัติได้จริง บุคลากรด้านไซเบอร์มีประสิทธิภาพพร้อมรับภัยคุกคามด้านไซเบอร์ที่นับวันจะทวีความรุนแรงและถูกยกระดับให้กลายเป็นพลังอำนาจแห่งชาติที่สามารถทำให้เกิดผลกระทบอย่างรุนแรงต่อความมั่นคงของชาติได้

4) การคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล มีอิทธิพลโดยตรงต่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ซึ่งสอดคล้องกับ Urciuoli L. (2013) ทำการศึกษาโดยพบว่า กลยุทธ์การจัดการความเสี่ยงและการคืนสภาพได้ของ โซ่อุปทานดิจิทัล มีบทบาทสำคัญในการสร้างความมั่นใจในความการจัดการความต่อเนื่องทางธุรกิจ และความน่าเชื่อถือในลักษณะของการประหยัดต้นทุน การป้องกันหรือการกู้คืนจากการหยุดชะงักของระบบ ต้องการการเข้าถึงและการวิเคราะห์ข้อมูลจำนวนมาก ๆ ดังนั้น จากการที่มีผลประโยชน์สำหรับผู้ที่มีส่วนได้ส่วนเสียจากการดำเนินงานและบริบทด้านต่าง ๆ ที่เกี่ยวกับโซ่อุปทานดิจิทัล จึงต้องทำการคืนสภาพได้ทางไซเบอร์อันเป็นสิ่งที่ท้าทายในการสร้างความต่อเนื่องทางธุรกิจต่อโซ่อุปทานดิจิทัล เช่นเดียวกับการศึกษาของยุทธนา เจียมตระการ (2561) ศึกษาเรื่อง การจัดการความมั่นคงปลอดภัยไซเบอร์ สำหรับอุตสาหกรรมขนาดใหญ่ การศึกษาพบว่า แนวทางการสร้างความมั่นคงปลอดภัยไซเบอร์ขององค์กรสำหรับอุตสาหกรรมขนาดใหญ่ ประกอบด้วยประเด็นสำคัญคือ 1) การตระหนักถึงในเรื่องการสร้างความมั่นคงปลอดภัยไซเบอร์จากผู้บริหารระดับสูง ที่ต้องทราบถึงผลกระทบของภัยคุกคามไซเบอร์ที่จะสามารถทำให้องค์กรหยุดชะงักซึ่งจะมีผลต่อกระบวนการการผลิตและกระบวนการทาง

ธุรกิจได้ 2) ความจำเป็นที่องค์กรจะต้องมีกลไกสำหรับการบริหารจัดการความเสี่ยง และต้องมีการใช้กลไกดังกล่าวเพื่อนำไปประเมินผลกระทบในภาพรวม อันจะนำไปสู่การกำหนดนโยบายเกี่ยวกับการสร้างความมั่นคงปลอดภัยไซเบอร์ การปรับโครงสร้างการจัดการภายในองค์กร การกำหนดผู้รับผิดชอบทั้งในรูปแบบหน่วยงานหลัก และในรูปแบบคณะกรรมการ เพื่อขับเคลื่อนนโยบายสู่การปฏิบัติ 3) องค์กรควรจะต้องนำผู้เชี่ยวชาญระดับสากลมาทำการตรวจประเมิน ในเรื่องของการบริหารจัดการและการดำเนินการทางด้านความเสี่ยง ที่เป็นอยู่ในองค์กร เพื่อจะทำให้ทราบถึงจุดเสี่ยงจากภัยคุกคามไซเบอร์และนำไปสู่การจัดทำแผนยกระดับความมั่นคงปลอดภัยไซเบอร์ โดยต้องมีการพิจารณาถึงความพร้อมและความสำคัญเร่งด่วนภายใต้ความเสี่ยง และบริบทขององค์กรควบคู่กันไป จำเป็นต้องมีการสร้างความมั่นคงปลอดภัยไซเบอร์ได้เป็นกรอบดำเนินการภาพใหญ่ และมีการกำหนดถึง กรอบการดำเนินงานโดยอาจเพิ่มเติมกิจกรรมลงในแต่ละกรอบย่อยได้ตามบริบทของธุรกิจ นอกจากนี้ยังพบถึงปัจจัยภายนอกและภายในที่ช่วยเร่งให้เกิดประสิทธิผลและประสิทธิภาพใน การจัดการความเสี่ยงขององค์กรได้ โดยปัจจัยภายนอก ได้แก่ นโยบายของภาครัฐ กฎหมายด้านไซเบอร์ การสร้างบุคลากร เครือข่ายความร่วมมือ และปัจจัยภายใน ได้แก่ วิสัยทัศน์และภาวะผู้นำและการเตรียมพร้อมรับมือ

5) จากผลการศึกษาโมเดลปัจจัยตัวแปรเชิงสาเหตุที่ส่งผลต่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล พบว่าความร่วมมือกันของโซ่อุปทานดิจิทัล การจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล และการจัดการความเสี่ยงทางไซเบอร์ของโซ่อุปทานดิจิทัล เป็นปัจจัยที่มีผลต่อการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัลรวมไปถึงความร่วมมือกันของโซ่อุปทานดิจิทัล และการจัดการภัยคุกคามทางไซเบอร์ของโซ่อุปทานดิจิทัล เป็นปัจจัยที่มีผลต่อการจัดการความทางไซเบอร์ของโซ่อุปทานดิจิทัล อีกทั้งการคืนสภาพได้ทางไซเบอร์ของดิจทัลซัพพลายเชนยังเป็นปัจจัยที่ส่งผลต่อการจัดการความต่อเนื่องทางธุรกิจ

5.3 ปัญหาอุปสรรคและข้อจำกัดของการวิจัย

1. ปัญหาและอุปสรรคของการวิจัย พบว่าการศึกษาวิจัยและพัฒนาตัวแบบวุฒิภาวะใด ๆ ก็ตาม จำเป็นอย่างยิ่งที่ต้องได้รับข้อมูลพื้นฐานเกี่ยวกับแนวทางการปฏิบัติในเรื่องนั้น ๆ อย่างเจาะลึกจากผู้มีประสบการณ์ ตลอดจนผู้เชี่ยวชาญ จำนวนมากทำให้ใช้เวลาในการเก็บรวบรวมข้อมูลโดยส่วนใหญ่จะเป็นข้อมูลเชิงคุณภาพ รวมถึงขั้นตอนสกัดข้อมูล ขั้นตอนการดำเนินการวิจัยในส่วนนี้จะใช้เวลาในการเก็บข้อมูลและวิเคราะห์ข้อมูลค่อนข้างใช้ระยะเวลานานพอสมควร

2. ปัญหาและอุปสรรคอีกประการหนึ่งของงานวิจัย พบว่าการเก็บรวบรวมข้อมูลจากผู้ประกอบการจะเป็นไปได้ค่อนข้างยาก เพราะส่วนใหญ่ผู้ประกอบการ SME จะยังไม่เห็นความสำคัญของการโจมตีจากทางไซเบอร์เท่าไหร่นัก อาจจะมองในแง่ของการลงทุนทางด้านไอทีที่ค่อนข้างสูง ผู้วิจัยได้พยายามชี้แจงถึงความสำคัญ และความจำเป็นที่ผู้ประกอบการจะต้องเตรียมรับมือ และชี้ให้เห็นว่าเครื่องมือที่ผู้วิจัยทำนั้นเป็นเพียง Self Assessment ที่ไม่ต้องลงทุนไปจ้างผู้เชี่ยวชาญมาทำการสำรวจ ความพร้อมขององค์กร หรือแม้แต่กระทั่งผู้ประกอบการรายใดที่ต้องการจะพัฒนาระบบงานตัวเองให้มีมาตรฐานสากลในด้านความมั่นคงปลอดภัยทางไซเบอร์ จะได้ทราบถึงปัญหาของตัวเองก่อน ก่อนที่ลงทุนจ้างผู้เชี่ยวชาญเข้ามาประเมิน เพื่อปรับปรุงและพัฒนาระบบงานขององค์กรต่อไป

3. ข้อจำกัดของงานวิจัย พบว่าการศึกษาในครั้งนี้ได้นำเสนอตัวแบบวุฒิความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม ซึ่งยังอยู่ในขั้นตอนของการออกแบบ (Design) จำเป็นต้องอาศัยการศึกษาเพื่อพัฒนาในขั้นตอนของการตรวจสอบต่อไปในอนาคต

4. เนื่องจากประชากรและกลุ่มตัวอย่างผู้วิจัยได้ใช้วิสาหกิจขนาดกลางและขนาดย่อมที่ไม่ได้ชี้เฉพาะในรายภาคธุรกิจเพื่อการศึกษา อาจจะทำให้ตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัลจึงไม่อาจจะจะสามารถแก้ปัญหาได้ในทุกภาคธุรกิจของวิสาหกิจขนาดกลางและขนาดย่อม แต่การพัฒนาตัวแบบผู้วิจัยเพียงแต่ต้องการให้เกิดแนวทางในการพัฒนาตัวแบบเพื่อให้วิสาหกิจขนาดกลางและขนาดย่อมได้เตรียมความพร้อมเพื่อรับมือต่อภัยคุกคามทางไซเบอร์ที่อาจจะเข้ามาได้อยู่ตลอดเวลา

5.4 ข้อเสนอแนะ

1. ข้อเสนอแนะสำหรับการนำผลการวิจัยไปใช้งาน

1.1 จากผลการวิจัยที่ได้กรอบแนวคิด ตัวชี้วัด ทำให้สามารถเห็นแนวทางในการปฏิบัติเพื่อประยุกต์ใช้การคืนสภาพได้ทางไซเบอร์ในด้านการบริหารงานทางด้านโลจิสติกส์และโซ่อุปทานได้อย่างเป็นรูปธรรม สามารถนำไปปฏิบัติจริงได้

1.2 ผลการวิจัยนี้สามารถใช้เป็นแนวทางเพื่อนำไปพัฒนาให้แก่วิสาหกิจขนาดกลางและขนาดย่อมในแต่ละด้าน หรือเฉพาะด้าน หรือเฉพาะกลุ่มอุตสาหกรรมต่อไปได้ เพื่อที่จะสามารถนำระบบประเมินที่ได้พัฒนาขึ้นนี้ไปพัฒนาและประยุกต์ใช้ภายในองค์กรของตนเองได้

1.3 ควรมีการประยุกต์ใช้ตัวแบบวุฒิภาวะและตัวชี้วัดที่พัฒนาขึ้น ไปสู่องค์กรหรือบริษัท หรือภาคอุตสาหกรรมขนาดใหญ่ โดยเฉพาะอย่างยิ่งองค์กรมหาชน ที่อยู่ในตลาดหลักทรัพย์

ที่ต้องให้ความสำคัญอย่างมากในการนำหลักการคืนสภาพได้ทางไซเบอร์ไปใช้ในองค์กร และทำการขยายผลเพื่อปรับใช้ให้เหมาะสมกับองค์กร ซึ่งองค์กรสามารถที่จะทำระบบการประเมินเป็นเพื่อให้เห็นสภาพของระดับวุฒิภาวะ ด้วยการประเมินทีละมิติ หรือทีละตัวชี้วัด ขึ้นอยู่กับความต้องการขององค์กร ซึ่งระบบมีความยืดหยุ่นเพียงพอที่จะสามารถตอบสนองความต้องการประเมินในแต่ละรูปแบบได้

2. ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

2.1 ควรศึกษาแนวปฏิบัติการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทาน เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในบริบทขององค์กรที่แตกต่างออกไป โดยสามารถใช้ผลการศึกษาของงานวิจัยฉบับนี้เป็นฐานและศึกษาเปรียบเทียบความเหมือนหรือแตกต่าง เพื่อขยายผลให้ได้ตัวแบบที่มีความเฉพาะ (Specification) ต่อองค์กรมากยิ่งขึ้น ซึ่งจะทำให้เกิดความเหมาะสม (Fit) ในการนำไปใช้จริงมากยิ่งขึ้น

2.2 ควรศึกษาเพื่อพิสูจน์หรือทดสอบตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม ที่ได้นำเสนองานวิจัยฉบับนี้ ในด้านการศึกษาอิทธิพลของตัวชี้วัดที่มีต่อระดับ (Level) ต่าง ๆ ของระดับวุฒิภาวะ

2.3 ควรศึกษาเพื่อพิสูจน์หรือทดสอบตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม ที่ได้นำเสนองานวิจัยฉบับนี้ เกี่ยวกับผลกระทบของตัวแบบต่อองค์กรเมื่อมีการนำไปประยุกต์ใช้จริง ในด้านการยอมรับตัวแบบ โดยอาจจะใช้ตัวแบบการยอมรับเทคโนโลยี (Technology Acceptance Model: TAM) มาเป็นฐานในการทดสอบ

2.4 ควรศึกษาเพื่อพิสูจน์หรือทดสอบตัวแบบวุฒิภาวะความสามารถการคืนสภาพได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม ที่ได้นำเสนองานวิจัยฉบับนี้ เกี่ยวกับผลกระทบของตัวแบบต่อองค์กรเมื่อมีการนำไปประยุกต์ใช้จริง ด้านประสิทธิภาพการดำเนินงานขององค์กรในภาพรวม ได้แก่ ความยั่งยืนการเติบโตขององค์กร คุณภาพของการให้บริการ การวิจัยและพัฒนาการแตกขยายองค์กร เสถียรภาพทางการเงิน การอนุรักษ์ทรัพยากร เป็นต้น ว่าตัวแบบที่พัฒนาขึ้นมีความขัดแย้งหรือสนับสนุนมาเจริญเติบโตขององค์กรอย่างไร

2.5 การนำองค์ประกอบหรือตัวชี้วัดอื่น ๆ อาทิเช่น ดัชนีความยั่งยืน ประสิทธิภาพในการดำเนินงาน มาเป็นตัวแปรตามเพื่อดูผลกระทบตัวแบบวุฒิภาวะความสามารถการคืนสภาพ

ได้ทางไซเบอร์ของโซ่อุปทานดิจิทัล เพื่อการจัดการความต่อเนื่องทางธุรกิจดิจิทัล ในวิสาหกิจขนาดกลางและขนาดย่อม ที่ได้นำเสนอ ว่าผลขององค์ประกอบหรือตัวชี้วัดเหล่านั้นจะทำให้เกิดประสิทธิภาพในการดำเนินงานขององค์กรหรือไม่และอย่างไร หรือ เพื่อให้เกิดการผลลัพธ์ที่ข้อค้นพบใหม่ ในด้านของอิทธิพลของตัวแบบที่มีต่อตัวแปรใหม่ ๆ

2.6 มิติความต่อเนื่องทางธุรกิจ (Continuity) เป็น อีกหนึ่งมิติที่น่าสนใจ และสามารถทำวิจัยต่อยอดเพื่อขยายองค์ความรู้ได้มากมายโดยเฉพาะการทำให้องค์กรสามารถคืนสภาพได้อย่างรวดเร็วเมื่อเกิดภัยคุกคามหรือการโจมตีทางไซเบอร์ อาจจะกระทำได้โดยการศึกษาถึงแนวปฏิบัติที่ดีของแต่ละองค์กร เพื่อการนำพาธุรกิจไปสู่การคืนสภาพได้ทางธุรกิจ (Business Resilience) ภายใต้ธุรกรรมดิจิทัลที่จะเกิดขึ้นต่อไปในอนาคต